Upskilling to Upscale:

Unleashing the Capacity of Civil Society to Counter Disinformation

EXPOSE NETWORK SCOPING – FINAL REPORT
JUNE 2018

CONTENTS

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXES

1. EXECUTIVE SUMMARY

Europe is under an increasing threat from Kremlin-backed disinformation. The Kremlin aims to contaminate the information ecosystem in order to destroy foreign governments' reputations, weaken international alliances, increase polarisation, undermine trust in government and other major institutions, influence political and in particular electoral outcomes and, ultimately, enhance Russian global influence.

These disinformation efforts are proving successful across Europe due to the fact they exploit existing fissures and debates in society, require low barriers to entry, are able to circumnavigate a weak regulatory environment, and exploit low levels of public awareness and a lack of critical media consumption. The rise of 'deep fake' technology and other tools for image and video manipulation is an additional urgent concern.

There is a pressing need to counter disinformation with high quality, credible content that exposes and counters false narratives in real time and builds resilience over the long term among populations vulnerable to Kremlin influence. The complexity of Kremlin-backed disinformation and its regional nuances requires a response that is regionally based and adaptive to local scenarios, but also draws on a broader understanding of the Kremlin's strategic goals.

Due to the scale and gravity of the threat across Europe, there are an increasing number of organisations with a high commitment to understanding and countering Kremlin-backed disinformation, often doing so in the face of strong opposition and with little remuneration or support for their work. Civil society organisations are uniquely placed to counter Kremlin disinformation as they have the commitment, mission and potentially the credibility to not only counter disinformation but also build long-term resilience to it through positive messaging, improving regulation and building awareness and critical thinking amongst the public.

This scoping research included an in-depth analysis of existing organisations around Europe countering disinformation using a variety of tactics including public awareness campaigns, the development of tech tools, the development of research products, and open source research into the networks and sources of disinformation. These organisations include media outlets, think tanks, and grassroots implementors running projects that include promoting media literacy and community cohesion. It found that despite significant achievements in the fields of fact-checking and debunking, research, public facing campaigns, network analysis, investigative journalism and media literacy, there are core weaknesses that undermine the ability of organisations to effectively counter disinformation.

The majority of these organisations are operating completely independently in a disparate fashion without sharing best practice. Their outputs have varying degrees of quality and effectiveness, and are not informed by the latest data and research, and they have limited operational capacity to do this work at the pace and scale required.

An opportunity exists to upskill civil society organisations around Europe, enhancing their existing activities and unleashing their potential to effectively counter disinformation. If supported to deliver their activities in a professional manner that holds them above reproach, while gaining access to a variety of support functions, best practice and high-quality training these organisations have the potential to be the next generation of activists in the fight against Kremlin disinformation.

EXECUTIVE SUMMARY

The EXPOSE Network sets out to identify civil society organisations operating across Europe countering disinformation using a variety of tactics, upskill these organisations in research and communications and through the provision operational support, grants and training, and coordinate their activities to ensure effectiveness and measure impact through research and evaluation.

Four key barriers to countering disinformation effectively can be identified across the region as a whole. Organisations lack:

- The expertise, guidance and tools to deliver high-quality open source research
- The ability and support to conceptualise and deliver public facing campaigns and communications products that challenge public perceptions about disinformation
- Access to grant funding, relationships with donors, and the ability to write funding proposals, severely limiting their sustainability, as well as qualified staff
- The security frameworks and legal training to run streamlined and low-risk operations

The operating model proposed will address these key barriers highlighted through the provision of five activity strands. These will run in parallel throughout the three-year implementation period. Resourcing will include a grant funding mechanism, and will ensure that organisations have access to legal, security and other operations support to enable them to deliver their work within a safe and well-resourced environment. Training will include a variety of learning packages, from online courses to embedded learning with dedicated specialists and regional events focused on topics including cyber security and enhancing communications outputs. Research and evaluation of impact will involve both a study of disinformation as it emerges online and the evaluation of the activities of network members to better understand their impact on the target audiences. Coordination of activities and network members will foster synergies between research interests, promote regional cooperation, and facilitate networking, as well as drawing together activities and promoting specific approaches if necessary. The Quality Assurance (QA) strand will ensure that wherever possible outputs from Network members are created within rigorous journalistic, fact-checking and legal frameworks and will drive to increase quality in both research and communications.

In delivering activities across the five strands of resourcing, training, QA, coordination of activities, and research and evaluation of impact, the Network Facilitator will achieve a joined-up approach that matches technical training with the provision of funds and tools, ensures activities are not only delivered to a high standard but coordinated in order to achieve maximum impact, and provides a crucial layer of impact measurement to all the work undertaken by Network members.

This will in turn increase the quality and quantity of counter-disinformation content, increase the sustainability and professionalism of organisations countering disinformation, create an ecosystem of credible voices which can continue to grow and counter the disinformation ecosystem exploited by the Kremlin, build awareness amongst key audiences, and help to establish best practice on countering disinformation. These outputs will contribute to the undermining of the credibility of the Kremlin, their narratives and online networks, build resilience to disinformation in vulnerable audiences across Europe, and reduce the number of unwitting multipliers of disinformation.

The upskilling of civil society organisations across Europe represents a unique opportunity for the FCO to adopt a joined-up approach, ensuring information sharing between the private sector, civil society and Government while enabling civil society organisations to counter disinformation in a way that matches the challenge in their local contexts.

2. UNDERSTANDING DISINFORMATION

2.1. DEFINITIONS

In this report, 'disinformation' refers to Kremlin influence operations within the communications environment, delivered through overt and covert promotion of intentionally false, distorting or distracting narratives. Kremlin influence operations form part of a much broader foreign policy toolkit, which includes the use of official and illicit money, corruption, economic pressure, assassinations, online hacking, political party funding, support for extremist movements and the use of the Orthodox Church and state-controlled NGOs in foreign policy.

This project scoping has taken a broad approach to disinformation both in the way it can be understood and in approaches to countering it.

2.2. STRATEGY AND TACTICS

The Kremlin aims to contaminate the information ecosystem in order to destroy foreign governments' reputations, weaken international alliances, increase polarisation, undermine trust in government and other major institutions, influence political and in particular electoral outcomes and, ultimately, enhance Russian global influence. The Kremlin's objectives and tactics are summarised in the following table:

INTENT	STRATEGY	EXAMPLE
DESTROY FOREIGN GOVERNMENTS' REPUTATIONS	Inventing/promoting smear campaigns and alternative narratives through Kremlin-attributed media and Kremlin public diplomacy. Promoting these narratives by non-attributed and attributed Kremlin activity. Using troll/bot networks to swamp and distort discussion.	Smear campaign against the White Helmets, a group trusted by the UK government, especially their evidence of the use of chemical weapons by Russia and its allies in Syria. Corroding confidence in the UK's political system through bringing into question the integrity of the Scottish independence referendum.
WEAKEN INTERNATIONAL ALLIANCES	Creating campaigns inventing or highlighting decadence, corruption, hypocrisies or decay of institutions. Promoting these narratives through both non-attributed and attributed Kremlin media / social media.	Creating multiple false narratives to reject the UK government's analysis of the poisoning of the Skripals in Salisbury or muddying the waters around the shooting down of the MH17 airliner by Russian-controlled forces in Ukraine.

UNDERSTANDING DISINFORMATION

INTENT	STRATEGY	EXAMPLE
DISTORT NATIONAL POLITICAL DISCOURSE TO PROMOTE RUSSIAN INTERESTS / BOOST INDIVIDUALS AND ORGANISATIONS WHO SERVE RUSSIAN PURPOSES	Promoting pro-Kremlin topics on RT/Sputnik (and via RT/Sputnik social media channels). Inserting Kremlin narratives into the mainstream media through the use of public diplomacy. Using troll/bot networks to swamp and distort discussion. Deployment of campaigns through troll/bot networks to divert energy and attention from discussing Kremlin activity. Championing of third-party advocates to simulate credibility to Kremlin narratives.	Disinformation campaign aimed at Russian minorities in Eastern Europe, and Slavic and Christian Orthodox 'brethren' in South Eastern Europe with historical ties to Russia, in order to galvanise domestic pressure for stronger links to Russia. In Serbia, Kremlin disinformation has instilled the false idea that the Kremlin offers more investment into the Balkans than the EU.
UNDERMINE TRUST IN PUBLIC INSTITUTIONS	Amplifying anti-government voices. Undermining key institutions such as public service broadcasters. Promoting narratives about the economic or military unviability of a government. Increasing divisions between minority communities and their government.	Narratives that Ukraine is economically a failed state and can only survive if it is propped up by the EU or Russia. Smear campaign against the BBC. Narratives in Baltics that Russian speakers are persecuted by the government.
INFLUENCE ELECTORAL AND POLITICAL OUTCOMES	Promoting candidates or discrediting others in order to achieve specific outcomes.	Disinformation campaigns interfering in US elections, Italian elections, Catalan independence referendum.
INCREASE POLARIZATION	Amplifying existing far-left and far-right narratives on social media through providing fodder for consumption and opinion entrenchment. Using troll/bot networks to swamp and distort discussion, making the narratives 'unavoidable' on social media. Manipulating far right groups, far left groups, anti-Zionists, conspiracy theorists, Kremlin sympathisers, and critics of the mainstream media, who opportunistically amplify content produced by fringe networks moving them from 'Kremlin-narrative observers' to 'Kremlin-narrative contemplators/sympathisers/amplifiers'. Fringe networks sharing this content used key mainstream hashtags when amplifying content, resulting in fringe network activity bleeding into the mainstream.	Stoking ethnic and religious hatred following the terror attacks in the UK and France in early 2017. Creating alarmist stories about mass migration into Germany, and across the EU generally. Inflaming the situation around Catalan separatists during the 'independence' vote.

These disinformation efforts are proving successful across Europe due to the fact they:

- Exploit existing fissures and debates in society. Disinformation mobilises existing communities of interest both online and offline, including those who are already alienated from the mainstream for a variety of reasons, including the legacy of the disintegration of the Soviet Union and existing ethno-political tensions.
- Require low barriers to entry. The technical tools necessary to create and disseminate disinformation are easily accessible and require low levels of ability and cost to produce at high volume. The rise of tools for image and video manipulation, including 'deep fakes', is an additional factor that will increase the Kremlin's ability to create credible disinformation.
- Circumnavigate a weak regulatory environment. The Kremlin's tactics are playing out in a context where the introduction of digital media has led to new forms of influence campaigns waged by all political and commercial actors, around which there exists little or no regulation or norms. There are few existing frameworks and little public awareness around how the public's online data can be used by technology companies, or around what constitutes legitimate political advertising online or what forms of digital amplification (such as Search Engine Optimisation or the use of automated accounts) are legitimate.
- Exploit low levels of public awareness and a lack of critical media consumption.

There is a pressing need to counter disinformation with high quality, credible content that exposes and counters false narratives in real time and builds resilience over the long term among populations vulnerable to Kremlin influence.

2.3 REGIONAL ANALYSIS

The scope of this research was Europe, with a focus on the areas prioritised by the FCO. The strategy and tactics implemented by the Kremlin in each territory are varied and shifting, and it is therefore important to take a local and contextually specific approach to both understanding and countering disinformation.

2.3.1 BALKANS

These countries face a 'dual threat' from Kremlin disinformation and from local media which echoes Kremlin narratives, and which are in some cases supported by the Kremlin. Narratives aim to pull countries away from the EU and NATO, to stir ultra-nationalism, and to destabilise peace efforts. In neighbouring countries, disinformation is partnered with attempted coups, the alleged training of paramilitaries and the subversion of election results.

For example, in Bulgaria there are a large number of narratives pushed by the Kremlin, including the moral and political decline of Europe, and conspiracy theories about the refugee crisis being a United States/CIA plot. The European Union is routinely subject to scrutiny. At times, stories portray Brussels as a malevolent prime mover, while at others, the EU is depicted as being a puppet of foreign governments and corporate interests, with George Soros featuring prominently.

2.3.2 BALTICS

In the Baltic states, disinformation efforts primarily target Russian-speaking populations, who are more naturally drawn toward the Kremlin's sphere of influence. Russian state TV is popular and supported by online and offline media in titular languages, including the recent launch of Sputnik in Lithuanian. Disinformation aims to polarise countries along ethnic and linguistic lines, furthering a sense of grievance among Russian speakers. Narratives are also aimed at discrediting the EU and NATO, with NATO soldiers a particular target for disinformation.

2.3.3 CENTRAL EUROPE

Kremlin disinformation plays into local political dynamics, preying on far-left and far-right narratives, particularly anti-immigration and anti-EU themes. These dovetail with narratives pushed by some heads of government, who in turn support Kremlin interests. In addition, internet news resources with opaque ownership push Kremlin narratives in a structured and strategic manner.

An example of this can be seen in the Czech Republic where two cross-cutting issues exploited by the Kremlin are negative attitudes towards migration, especially from Muslim countries, and negative sentiment towards the EU; these are also exploited by far right groups. A similar pattern was also observed in Hungary, where disinformation spreads far-right narratives about migration, liberalism and the EU.

2.3.4 CAUCASUS

In the Caucasus, Kremlin narratives are imported via the church, ethno-nationalist and anti-LGBT NGOs. Their aim is to push Georgia away from pursuing policies which align it to the EU and to weaken Georgian cooperation with NATO.

2.3.5 EASTERN EUROPE

In Ukraine, Kremlin legacy media and digital media still makes inroads, despite bans on Russian TV and social media companies. Its aim is to stir unrest and alienate Ukraine from its Western allies by, for example, inflaming Poland-Ukraine tensions.

Belarus and Moldova operate in a 'dual threat' environment. The Moldovan government pays lip service to the West by, for example, enacting an anti-propaganda law that purportedly banned propagandist outlets but simultaneously placated Russia by excluding a number of Russian TV stations from the ban.

In Belarus, media freedom is severely restricted. In Moldova, disinformation narratives cut across several key issues. The notion that if Moldova joins the EU then churches will be closed and Christian burials will be banned because European countries are not religious has gained prominence. Like in the Balkans, the prospect of being forced to support LGBT rights by Europe is used to turn people against the European project.

2.3.6 SOUTHERN EUROPE

The Kremlin uses Spanish-language disinformation to reach audiences in Southern Europe and further afield in Latin America and the United States. Disinformation spreads through Kremlin Spanish language broadcasters and across social media networks, where Kremlin accounts work in concert with Venezuelan ones. Narratives have included support for Catalan independence and support for Russian military interventions in Ukraine and Syria.

2.3.7 WESTERN EUROPE

Disinformation campaigns in Western Europe support far right and far left movements, fuelling polarisation. In the UK and elsewhere, disinformation is also spread to support Russian foreign policy objectives, including assassinations and invasions, to interfere in elections, and to attack politicians and influential individuals seen as unfavourable to the Kremlin. It is also deployed in the wake of terror attacks to promote hatred and increase social polarisation.

The complexity of Kremlin-backed disinformation and its regional nuances requires a response that is regionally based and adaptive to local scenarios, but also draws on a broader understanding of the Kremlin's strategic goals.

3. RESPONDING TO DISINFORMATION

Stakeholders from across society, including governments, the private sector and civil society organisations, are all engaged in responding to disinformation, with varying degrees of success. This scoping research analysed a wide range of tactics in order to gain a full picture of the impact, strengths and weaknesses of different approaches. Through extensive consultation with experts in the field and a literature review, we divided the range of approaches to tackling disinformation into six key strands, which are discussed in depth below.

3.1 TYPES OF RESPONSE

3.1.1 FACT-CHECKING AND DEBUNKING

This activity has a long tradition. During the Cold War, the US Government's inter-agency Active Measures Working Group tracked Soviet disinformation across the world, produced regular reports for Congress and communicated results to the press. The Working Group helped raise awareness of Soviet techniques among policy and media actors, which contributed to a broader narrative which undermined Soviet credibility.

The speed of production and distribution of content makes this a challenging endeavour in the present day. The media environment is no longer mediated by a handful of regulated outlets, and many content providers have no professional, commercial or regulatory interest in engaging with mythbusting. Furthermore, the fracturing of audiences means that vulnerable groups can be harder to reach, with an increasing body of research indicating that 'debunking' can in fact lead to unintended or even opposite results.[1]

Fact-checking institutions have grown rapidly across Europe, with the best ones signing up to the Poynter code of conduct and standards. Some of the most professional organisations are in Western Europe and areas with a strong Western donor presence, such as the Balkans. Central Europe is sorely lacking in this specialisation. Most fact-checking organisations however do not necessarily focus on the disinformation aspect, instead sticking to fact-checking politicians and mainstream media statements. Those organisations that do focus on debunking Kremlin fakes do not always follow the most rigorous standards.

The problems facing the sector can be seen in the complaints against the 'EU versus Disinformation' unit at the European External Action Service, which focus on questions of terminology and methodology. Though largely unfair, the complaints show how the lack of common agreement between researchers, academics and media on such questions can undermine the whole sector.

Despite these challenges, there have been notable incidents of fact-checking shifting public opinion and resulting in the source of a piece of disinformation backing down. There is huge potential here for civil society organisations to tread the path established by independent

[1] See Nyhan, B. and Reifler, J. (2010) 'When Corrections Fail: The persistence of political misperceptions', *Political Behaviour* 32: 303. https://doi.org/10.1007/s11109-010-9112-2; and Schmidt, A.K., Zollo, F., Scala, A., Betsch, C., and Quattrociocchi, W., (2018, May), 'Polarization of the vaccination debate on Facebook' in *Vaccine* https://www.ncbi.nlm.nih.gov/pubmed/29773322

social media users and media outlets. Fact checking can have a key role in stopping journalists and other trusted social media amplifiers and influencers from sharing disinformation content, and also from undermining the credibility of the sources of that content via drawing attention to the sources. Satire has been particularly effective in this regard, as the following case study shows:

CHANNEL ONE EURASIA FORCED TO BACK DOWN

In 2016, in the midst of widespread protests against the Kazakhstani government's proposed land reform legislation, Channel One Eurasia (the Channel One affiliate in Kazakhstan) broadcast a video that it claimed proved that foreign agents were funding the protest. The badly-shot, clearly fake video featured anonymous provocateurs stuffing money into back pockets of 'protesters'. Social media users responded by producing dozens of parody clips lampooning the fake video; many of these went viral under hashtags mocking Channel One. As a result of the social media uproar, several staff members at Channel One were fired, and a Russian producer returned to Moscow.

DELFI: DEMASKUOK PROJECT

Delfi, the largest fact checker in Lithuania has launched a pioneering project called 'Demaskuok' ('uncover'). Readers of the website are able to submit stories that they think might be inaccurate for Delfi journalists to fact-check. This arose from an awareness on the part of the organization that "false news and deliberate misinformation have become more common in global social networks." They hope that their project will stop the "spread of panic," and other real-world losses associated with disinformation.

3.1.2 RESEARCH

Research conducted in this space needs to include analysis of the type of content being spread and the narratives it pushes, analysis of the tools and methods through which it is disseminated, and the ways in which it is consumed by audiences.

Think tanks and academic institutions regularly conduct deep and comprehensive analysis of Kremlin narratives. Such research can raise awareness of the scope and strategy of Kremlin activities among policy makers and media elites. It is slow, however, and makes no effort to keep pace with an ever-evolving landscape. It also rarely includes monitoring of narratives in real-time using social media monitoring tools.

Organisations in Central Europe and the Baltics excel in this area, as do the more established Western European think tanks. Such in-depth research tends to be targeted very narrowly at the policy-making and expert community and does not provide a feedback loop into predicting and countering Kremlin campaigns. Other regions, including Southern Europe, are sorely lacking in a deep understanding of the Kremlin's strategies, which could be both a cause and effect of their governments' reluctance to confront this issue. A concerted, transnational research and public awareness effort is necessary to ensure it is at the top of the political agenda in all the regions affected by Kremlin disinformation.

Monitoring of Kremlin media, and of its impact, is irregular and often conducted privately or in-house by governments. Social media listening tools are only available to professional digital marketing companies; traditional media monitoring is conducted by credible organisations such as Detektor Media in Ukraine and Memo 98 in Slovakia, but the former only focuses on Ukraine while the latter works on discrete commissions.

The lack of publicly available consistent monitoring and impact assessment is a significant gap in the field, and one of the most urgent to redress. The sort of longitudinal focus groups necessary to gauge impact will require long-term investment.

GLOBSEC: STRATCOM PROGRAMME

Through its Stratcom programme, Slovakia-based GLOBSEC runs a series of high profile research projects such as its annual GLOBSEC Trends report, which maps the effects of disinformation on public attitudes through a series of opinion polls in the Czech Republic, Hungary, and Slovakia, three states vulnerable to Russian influence. This enabled them to compare public perceptions of the EU, NATO, and the role of the US in these countries over time. GLOBSEC serves as a model of what can be achieved when an organisation is given adequate funding. Their Stratcom programme is run by four people with external co-operators across the region.

3.1.3 PUBLIC CAMPAIGNS

Awareness-raising activities are of core importance as a tool for challenging the infiltration and spread of disinformation into the public consciousness. There are few organisations across Europe with the ability and resources to effectively design and deliver these, though there have been examples of successful campaigns which others could learn from.

There is huge potential here for upskilling the ability of organisations to conceptualise, deliver, monitor and evaluate campaigns that reach vulnerable audiences with information that challenges Kremlin narratives and undermines disinformation.

3.1.4

GLOBSEC: STRATCOM PROGRAMME

GLOBSEC launched an inventive and engaging campaign using social media in order to bring attention to the risks posed by disinformation. They used two of the most popular Slovak bloggers to create a false online flame-war, pitting their fans against each other. There were subtle clues that the fight was false, and after several days it was revealed that it was a hoax to show people how easy it is to be fooled if information is not checked properly.

The campaign achieved 1.2 million views in a country of 5 million; though it should be noted that there was some spill over into the Czech Republic. GLOBSEC assessed it as the most successful counter-disinformation campaign in the region.

NETWORK ANALYSIS

Any understanding of disinformation needs to take into account the networks through which narratives are spread and the digital techniques that are used to amplify them. Digital network analysis is at the cutting edge of evaluating disinformation, pioneered at academic institutions, digital marketing companies and select think tanks such as the Atlantic Council Digital Forensics Lab. It is now starting to be pursued by some media outlets such as El Pais. Private companies such as Graphika and Alto Data have experience mapping Kremlin and extremist networks for a variety of government and private clients. This mapping is key to both understanding the emerging field and for designing interventions.

> "In exposing Russian propaganda, you are fighting a ghost. If you approach counter disinformation without exposing the networks, you will fail."
>
> Bulgaria Analytica

Exposing networks of sources that spread disinformation, rather than trying to counter specific stories and pieces of content, may be one of the most effective and sustainable ways of countering disinformation. A preponderance of evidence shows that when people are confronted with information which challenges the beliefs or values they already hold they are most likely to reject the information and further entrench their position. However, sensitively highlighting sources which people have previously trusted and showing that they are attempting to malignly influence the conversation can activate a sense of being manipulated and act as an affront to an individual's deeper emotional and psychological need to see themselves as rational and informed.

In addition, nodes in disinformation networks tend to be active in multiple disinformation campaigns. For example, the Kremlin repurposed bot/troll accounts and exploited the same far left and far right communities for both the anti-White Helmets and pro-Brexit campaigns in the UK. Exposing this finite network of disinformation nodes can have a long term counter-disinformation impact.

However, the digital tools necessary for such research are expensive and available to few groups. There is an urgent need to proliferate tools among different organisations, to help with training on how to use them optimally and then pool research to understand Kremlin and pro-Kremlin networks. There is ample talent in many of these regions to develop this. Central Europe has excellent digital marketing companies and computer scientists, as have Ukraine and Belarus. Delfi has built a prototype for an Artificial Intelligence tool that tracks articles published by over 100 websites known to spread Russian disinformation, leading the way for research in that area.

DELFI: ARTIFICIAL INTELLIGENCE

Delfi has built a prototype for a web-based AI tool that currently tracks articles across over 100 websites that are known to publish disinformation in Russian and Lithuanian. The tool can classify articles published by these websites by popularity, keywords, social media shares, author, or countries mentioned. The tool is monitored by about 300 volunteers who flag stories they believe are inaccurate or false, and then publish articles debunking them on the website.

A full version of the tool is expected to be launched in late summer 2018. They hope to include other European languages and to add additional features, including the ability to subscribe to articles, an automated 'fake score," and a social media page and feed crawler.

3.1.5 INVESTIGATIVE JOURNALISM

Narrative-driven investigative journalism is increasingly proving an extremely powerful way to expose the Kremlin's disinformation. Spectacular scoops have been obtained by Western, and more importantly Russian, journalists: years before media in the US was paying attention to the Internet Research Agency, courageous Russian journalists had already unmasked it. In the Czech Republic, journalists have investigated the ownership structures behind opaque pro-Kremlin disinformation websites. The Baltics have excellent investigative journalistic outfits who have exposed Kremlin strategies in the region.

Investigative journalism is however expensive, dangerous and sporadic. For greater impact, investigative journalism into disinformation needs to become more transnational and work in tandem with anti-corruption and counter-extremist organisations to uncover the financial backers of disinformation, and their intersection with far-right movements. Investigative journalism in this field also needs to be popularised so it can reach a broader audience, for example through narrative television and other accessible formats.

When smaller organisations have been equipped and upskilled to use their contextual and linguistic expertise to research and expose the narratives used by the Kremlin in their specific territories, this has proven an effective way of revealing both Kremlin tactics and the specific falsehoods that are being spread to local, vulnerable audiences.

BELLINGCAT: MH17

Bellingcat, an online investigation website, was at the forefront of exposing what happened to the Malaysian airliner MH17. The website published photos that it alleged tracked the movement of a Russian missile linked to the downing of the aircraft. Its findings were examined by a Dutch-led team of investigators, who said that they had a 'considerable interest' in Bellingcat's research output. Bellingcat has since published a comprehensive report that outlines the circumstances surrounding the incident and has gone further than official investigators in naming suspects.

3.1.6 MEDIA LITERACY

Media literacy is a critical component of countering disinformation and increasing resilience among the general population over the long term. Several innovative projects are updating media literacy training for the digital era, including IREX's highly regarded 'Learn to Discern' program in Ukraine.

IREX: LEARN TO DISCERN

IREX, a global development and education organisation, designed and implemented a program called 'Learn to Discern' in Ukraine. It is intended to address the problems associated with citizens not being able to detect disinformation. It encouraged people to support independent, truthful and ethical journalism, while teaching them how to tell whether something was true or false, or manipulative.

An impact study showed that participants were 28% more likely to demonstrate sophisticated knowledge of the news media industry, 25% more likely to self-report checking multiple news sources, and 13% more likely to correctly identify and analyse a fake news story.

These efforts should be implemented within vulnerable populations, including the older generation, and could involve a multi-platform approach including online quizzes, games and TV shows, similar to the work of StopFake in Ukraine. Media literacy efforts represent a unique opportunity to involve sections of the population in active participation in fact-checking. This involves individuals learning through doing, and thinking critically about the media through their own active experiences rather than merely being told about potential distortions and the suspect provenance of the information they are consuming.

A range of tactics have proven effective in countering disinformation. These are utilised by organisations from media outlets to think tanks and grassroots implementers. A response must contain within its armoury a full range of tactics to be implemented at different times and in multiple contexts in response to an emerging and rapidly shifting threat.

3.2 CIVIL SOCIETY: THE THIRD LAYER IN THE FIGHT AGAINST DISINFORMATION

Countering disinformation must involve governments, the private sector, and civil society organisations. Each of these plays a unique role and must be working in parallel, achieving a joined-up approach.

Government responses to Kremlin influence operations in Europe and frontline states have on the whole been disjointed and responsive rather than pre-emptive. While some Western governments have started to signal concern around the issue, many remain unwilling to confront the Kremlin directly or have their own interests in amplifying a similar disinformation agenda. There is justified scepticism of the extent to which governments should get involved in any issues which touch on freedom of speech. Moreover, governments are limited by having to frame this issue purely in terms of 'foreign' campaigns against a 'domestic' information space, when the reality of today's mediascape is that these distinctions are increasingly blurred.

The role of the private sector is to drive innovation through investing in research and tools that can be used by a wide range of organisations, including media outlets and civil society as a whole.

The upskilling of civil society organisations across Europe represents a unique opportunity for the FCO to adopt a joined-up approach, ensuring information sharing between the private sector, civil society and Government while enabling civil society organisations to counter disinformation in a way that matches the challenge in their local contexts.

3.3 UPSKILLING TO UPSCALE: UNLEASHING THE CAPACITY OF CIVIL SOCIETY TO COUNTER DISINFORMATION

Due to the scale and gravity of the threat across Europe, there are an increasing number of civil society organisations with a high commitment to understanding and countering Kremlin-backed disinformation, often doing so in the face of strong opposition and with little remuneration or support for their work. These include media outlets, think tanks, and grassroots projects that promote media literacy or community cohesion elements.

Civil society organisations are uniquely well-placed in this field, as they have the commitment, mission and potentially the credibility to not only counter disinformation but also build long-term resilience to it through positive messaging, lobbying to improve regulation, and building awareness and critical thinking among the public. However, the majority of these organisations are operating completely independently of one another in a disparate fashion without sharing best practice. Their outputs have varying degrees of quality and effectiveness and are typically not informed by the latest data and research. Furthermore, they have limited operational capacity to do this work at the pace and scale required.

RESPONDING TO DISINFORMATION

An opportunity exists to upskill civil society organisations around Europe, enhancing their existing activities and unleashing their potential to effectively counter disinformation. If supported to deliver their activities in a professional manner, while gaining access to a variety of support functions, best practice and high-quality training, these organisations have the potential to be the next generation of activists in the fight against Kremlin disinformation.

OUR RESEARCH SUGGESTS THAT AN EFFECTIVE RESPONSE TO DISINFORMATION MUST BE:

- Neutral to tactics; able to adopt a variety of tactics in response to emerging threats.
- Organic; able to emerge spontaneously and adoptive of linguistic and cultural nuances.
- Data-driven; incorporating a strong feedback loop and aware of the latest narratives and how they are being spread.
- Rapid; able to mobilise at a fast pace in line with the fast-moving disinformation networks utilised by the Kremlin.
- Locally embedded but transnationally networked; utilising the local media context and existing media outlets to disseminate content alongside the ability to see and respond to the transnational reach of Kremlin campaigns.

4. STRATEGIC APPROACH

4.1 OBJECTIVES

The EXPOSE Network will involve identifying civil society organisations operating across Europe countering disinformation using a variety of tactics; upskilling these organisations in research and communications, and through the provision of operational support, grants and training; and coordinating their activities to ensure effectiveness and to measure impact through research and evaluation.

THIS WILL:

- Increase the quality and quantity of counter-disinformation content.
- Increase the sustainability and professionalism of organisations countering disinformation.
- Create an ecosystem of credible voices which can continue to grow and counter the disinformation ecosystem exploited by the Kremlin.
- Build awareness among key audiences, including policy makers, journalists, the general public, and influencers/amplifiers of Kremlin strategy, tactics and networks.
- Help establish best practice on countering disinformation.

THIS WILL CONTRIBUTE TO:

- Undermining the credibility of the Kremlin, their narratives and online networks.
- Building resilience to disinformation in vulnerable audiences across Europe.
- Reducing the number of unwitting multipliers of disinformation.

4.2 AUDIENCES

A holistic approach to countering disinformation will target a variety of audiences.

THESE INCLUDE:

- The wider public; through the dissemination of campaigns and exposing the networks and sources of disinformation. This would also take into account media literacy activities, increasing resilience among the general population.
- Governments; national and local governments as well as multilateral institutions through engagement, public affairs and advocacy.
- Policy makers; through coordinated research outputs network members will provide policy makers with a cohesive national and regional picture of disinformation and its impact, and typology of the narratives that are spread .
- Journalists and mainstream media outlets; through embedded investigative journalism projects and the mapping of networks and sources, network members will provide facts to journalists and mainstream media outlets that prevent falsehoods reaching the mainstream media.

4.3 KEY BARRIERS TO COUNTERING DISINFORMATION EFFECTIVELY

Through online surveys and face-to-face interviews with 43 organisations in 14 countries a number of critical barriers to countering disinformation effectively have been revealed. From the challenges of operating under governments that are pro-Kremlin to the challenges in raising funds to deliver long-term work, as well as a lack of access to digital tools and learning opportunities, four trends can be identified across the region as a whole. The operating model proposed will address the following key barriers:

- Lack of expertise, guidance and tools to deliver high-quality open source research.
- Lack of ability and support to conceptualise and deliver public facing campaigns and communications products that challenge public perceptions about disinformation.
- Lack of access to grant funding, relationships with donors, and the ability to write funding proposals, severely limiting their sustainability, as well as qualified staff.
- Absence of security frameworks and legal training to run streamlined and low-risk operations.

These are covered in more detail in ANNEX A: Needs Assessment Findings.

4.3.1 RESEARCH

While good-quality research is an integral part of countering Russian disinformation, the capability of the organisations to do this effectively varies greatly. Fact-checking, monitoring social media, open source research, and mapping propagandist networks were identified as crucial tactics.

The capacity to conduct long-term research projects and in-depth investigations was the strongest area identified within the potential partners. However, the lack of awareness or adherence to the International Fact-Checking Code of Principles and the National Union of Journalists (NUJ) Code of Conduct was a potential limitation.

Organizations in countries with governments that are resistant to free and open journalism were the weakest in this regard. However, organizations in countries that are on the frontline of Russian disinformation campaigns and have governments focused on combatting the threat, such as Poland and the Baltic states, were identified as the strongest with regards to ethical journalism standards. However, even here, organizations do not formally stick to principles. Rather, they use what they describe as common sense and multiple source corroboration of evidence. A similar trend was identified in Belarus and Moldova. Organizations in Southern Europe were aware of the Poynter fact-checking principles and NUJ Code of Conduct; however, like other organisations, they did not officially adhere to them.

Fact-checking was identified as particularly strong capability within organisations in the Baltics. However, the fact-checking capability of potential partners in other regions is limited. It was not that organizations could not do this effectively, but rather that they questioned its efficacy. StopFake was a notable exception.

The inability of organisations to monitor social media was a far more significant gap identified. None of the organisations interviewed were aware of online listening tools. Organisations in the Balkans, Central Europe and Eastern Europe were the weakest in this regard. The same pattern was noted with regards to data science capabilities.

The ability to map and monitor propagandist networks, while strong in Slovakia and the Czech Republic, is limited in the rest of the network. Organizations in Georgia, for example, expressed a desire to enter this area but noted that they did not have the resources.

BULGARIA ANALYTICA: DATA SCIENCE

As the use of algorithms and systems designed to extract knowledge and insight from data becomes an increasingly important part of the counter-disinformation toolkit, many organisations are keen to exploit this and to develop data science and AI capabilities.

Bulgaria Analytica has expressed frustration that they do not have data science capabilities on their team, despite Bulgaria being extremely resource-rich in terms of people with data science skills (an estimated 40,000 people in Bulgaria are writing software for US companies). Additional funding to employ individuals with data science skills and to develop their in-house capabilities would ensure that this skill set could be used to tackle the disinformation threat.

4.3.2 COMMUNICATIONS

The research output generated by the organisations is limited in its impact if it is not read and understood by the public. Therefore, public communication is an integral part of countering disinformation. There were clear discrepancies in the ability and willingness of organisations to communicate their findings externally.

Organisations in 'single-threat' environments, where pro-Kremlin disinformation comes from Russian-affiliated sources, were found to be far more capable in this regard than organisations in 'dual-threat' countries, where local media echoes Kremlin narratives. Organisations in countries with governments that are supportive of the counter-disinformation effort operate in a far more conducive environment. Some, including Stop Fake and Detektor Media, receive government support. However, even they are limited in their ability to reach vulnerable audiences, such as Russian-speaking minorities in non-Russian speaking countries.

Out of eleven Central European organizations interviewed, only one, Globsec, is successfully reaching sizeable audiences, and none is reaching the most vulnerable communities, namely avid consumers of Kremlin disinformation.

Many organisations only carry out counter-disinformation activities online. This means that older members of vulnerable communities do not come across their counter-disinformation work. In the whole Baltic region only one organisation, the National Centre for Defense and Security Awareness, carries out offline activities.

Organisations in 'dual-threat' environments face significant obstacles, as their governments are resistant to the work they are producing. For example, Euroradio is forced to broadcast to Belarus from Poland. Meanwhile, the biggest pro-Russian propaganda outlet in Bosnia is Radio Televizija Republike Srpske, a state media outlet. Organisations in this area therefore face a significant challenge from television broadcasters.

The reach of analysis done by think tanks and academic institutions is limited by a number of factors. Firstly, it is deep and comprehensive, meaning that reading it is time-intensive and it does not lend itself to being shared on social media. Moreover, some organisations are very resistant to broadcasting their work on Russian disinformation, as they believe that it will bring them unwanted attention.

MALDITO BULO: INSTAGRAM

While Maldito Bulo has had success in promoting their work to the 30-50 age bracket, they have struggled to attract readers that do not use Twitter or Facebook. In order to increase their younger readership, they have begun to use Instagram to engage this audience. However, they do not have the resources to provide their staff with formal training. Instead, younger staff members who use Instagram try to explain the platform to older members who do not. They only have 1,661 followers on Instagram, compared to 140,000 on Twitter. It is evident that with additional training on digital communications and brand building they could dramatically increase their millennial readership.

4.3.3 SUSTAINABILITY

Most organisations interviewed mentioned the difficulty of generating enough funding to carry out their activities as effectively as possible.

Very few organisations in the Baltics have any experience of writing funding proposals and most had no awareness of funding opportunities available in their region or further afield.

Some organisations, such as Fundacja Reperterów in Poland, have begun to explore the possibility of using digital communications to raise awareness of their fundraising activities. However, their digital capabilities are also limited. This example serves to illustrate how capacity building in one area could have positive results across the full range of required capabilities. Several of the organisations interviewed reported frustrations that their team were not able to dedicate themselves full-time to the effort to counter disinformation due to the need to seek additional employment.

4.3.4 OPERATIONAL SUPPORT

Many organisations will require significant legal advice and ongoing support, as currently they do not operate within a procedural framework. More than 80% of organisations surveyed do not have any anti-bribery and anti-corruption policy or code of conduct in place. Meanwhile, only 5% of organisations interviewed provide basic training in legal compliance. The Bribery Act 2010 could have far reaching implications for network members. While only a small percentage of organisations had faced allegations of bribery or corruption, there was no uniformity in how organisations thought such allegations should be dealt with.

Moreover, over 80% of the organisations do not have a written discrimination policy. This presents risks as it limits the ability of the organisation to ensure compliance to their duties under the Equality Act 2010. New GDPR legislation could create additional problems for the organisations. Less than half of them had trained their teams in how to comply with the legislation.

In terms of cyber security, many organizations did not have any information security policies in place or relied on very basic information security training. Of the organisations that did have an information security policy in place, only one reviewed it monthly, and most only reviewed it annually.

We found that the biggest weakness with regards to operational support found across the entire network was the subjectivity of risk management. Most organisations did not have a formal system for identifying and preventing risks, and instead responded in an ad hoc manner. Moreover, we found that some partners had not identified a framework for responding to a security breach, or a process for informing relevant stakeholders that one had occurred.

A significant area for improvement is the lack of consistency with regards to what devices are permitted in the workplace. Many partners allowed staff to bring their own devices into work, despite the risks posed from devices that are not centrally managed and are therefore easier to compromise. As a device being compromised could allow a threat-actor to access sensitive data relating to the network, strategies will have to be put in place to minimise this risk. There is also a threat from the compromise of data due to human error or intention. Many organisations have no systems in place to prevent their staff from removing data, and some do not vet their staff.

While working as part of a partnership, it is important that all organisations apply the same process to communicate a breach to client and affected parties. It is advisable that a central policy is determined to manage these scenarios.

LATVIAN ELVES:
WEAKNESSES IN CYBER SECURITY AND VULNERABLE TO ATTACK

The Latvian Elves desperately need capacity building with regards to cyber security. The Elves are predominantly volunteers that belong to a 180-person strong Facebook group, rather than formal staff. The volunteers engage in debates and discussions online in order to raise questions about disinformation. This makes them highly visible to malign actors. Although they create blacklists and grey-lists of accounts suspected of being pro-Kremlin trolls, they have still experienced cyber-attacks. Some members of the Facebook group have even been doxed.

(doxing: to search for and publish private or identifying information about an individual on the internet, typically with malicious intent)

Several key weaknesses exist across research, communications, sustainability and operational functioning. The model below sets out to bring together organisations in such a way as to effectively address these gaps and weaknesses.

4.4 OPERATING MODEL

The EXPOSE Network will bring together organisations from across Europe already committed to countering disinformation, increase their technical skills and provide holistic operational support to enable them to professionalise and upscale their activities. The Network Facilitator will coordinate these activities and gain valuable information about their impact, while also increasing the ability of organisations to better understand their own impact and to tailor their activities accordingly.

The Network Facilitator will be based in a low-risk European country, hosting a team of technical specialists able to travel regionally to support organisations depending on their strategy and the response the current geopolitical climate requires.

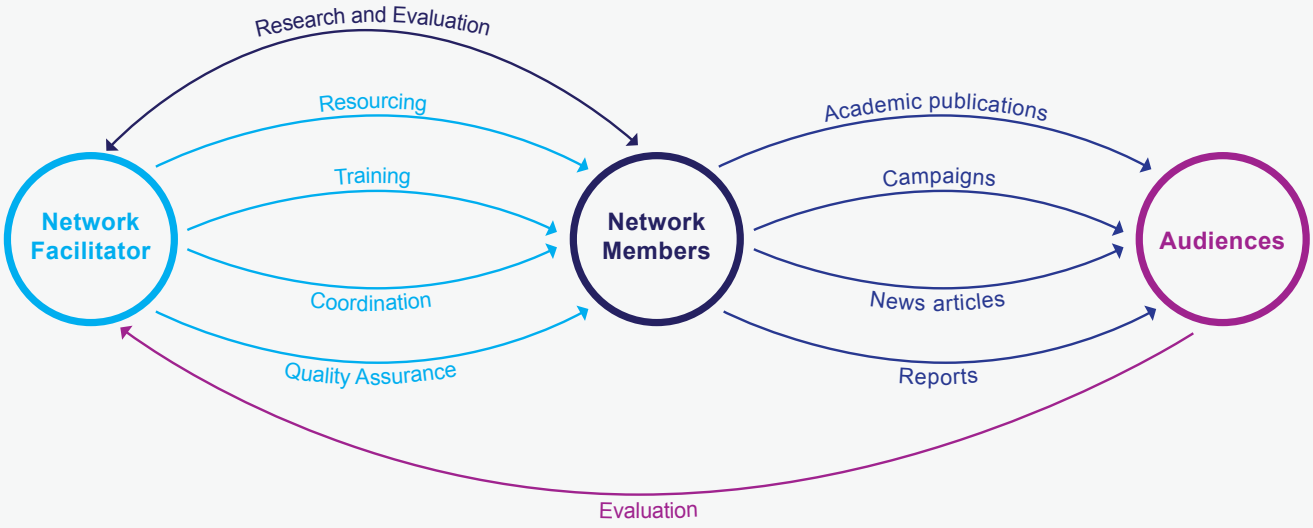
The network will be coordinated through a Central Hub run by the Network Facilitator. In addition to the organisations initially selected, membership will be open to new members on a rolling basis if they meet the initial criteria.

Membership of the network will provide training, tools and funding for research, and will facilitate transnational cooperation and public engagement. In turn, members will have to sign up to a mandatory code of ethics, standards and research methodologies, which will have to be maintained across any research carried out within the network.

The Network Facilitator will coordinate the activities of network members across borders, bringing together disparate implementations in order to streamline, ensure peer-to-peer learning, develop relationships between partners and measure effectiveness. It will also connect the Network's activities to parallel organisations looking at corruption and extremism issues, such as the OCCRP and OCCI.

The ongoing monitoring and evaluation will provide a comprehensive picture of activities happening across Europe and their impact on a micro and macro level, and will give the FCO the ability to coordinate activity in response to specific events or narratives being spread by Kremlin-backed media.

Figure 1: A diagram of the Network illustrating the relationships between the Network Facilitator, Network Members and Audiences



4.5 NETWORK MEMBERS

We recommend the Network encompasses a broad spectrum of organisations. The selection process has been designed to identify a longer list of potential network members spanning a variety of tactics to counter misinformation, and a broad subset of cross-cutting issues. The process has also taken into account the priority countries and regions set out by the FCO, representing a joined-up European-wide approach to combating misinformation from organisations that hold the most potential to do so.

The majority of potential network members included in this longlist are cognizant of efforts to counter disinformation and are already engaging in this space, but additional organisations have been included who have high potential due to their skill set or the issues they engage with. The organisations identified are, therefore, either already highly competent in some of the necessary tactics in the counter-disinformation sphere or display potential, given the right guidance and advice, to become highly effective actors in this arena.

Disinformation campaigns are often complex, and undertaken through a series of networks that feature both state actors and non-state actors with overlapping interests, some grounded in truth but disingenuously framed, others entirely false. Therefore, core to our approach is engaging with narratives and issues that intersect with Russian misinformation. We have selected organisations that are engaging with issues that might not be perceived at first glance to be Russian misinformation, for example far-right narratives, anti-migration narratives and pro-separatist narratives. **Organisations are also included who are combatting corruption, representing untapped potential in a core area that ties to disinformation.**

If the equipped network is employing a diverse set of tactics and engaging with a variety of cross-cutting issues and narratives, the Network Facilitator will be able to monitor how campaigns develop locally and across borders, and how they are effectively countered. Ultimately the data created by such a network showing the effectiveness of certain interventions will also become a lynchpin in designing and executing projects to measurably reduce and counter the impact of disinformation.

Some of these organisations are leaders in their fields, operating at scale and with globally recognised outputs, for example Bellingcat and DFR Lab, while others are smaller and still defining their offering, such as Bulgaria Analytica and Krik. The activities offered by the Network that each will want to participate in will therefore be different, and the potential for peer-to-peer learning is huge. Network partners such as DFR Lab could deliver training packages to smaller organisations as part of the scope offered by the Network Facilitator.

Each partner has been assessed for inclusion involving a comprehensive due diligence process (ANNEX B: Risk Management Framework), their track record in identifying and tackling disinformation, its reputation and mission statement and objectives.

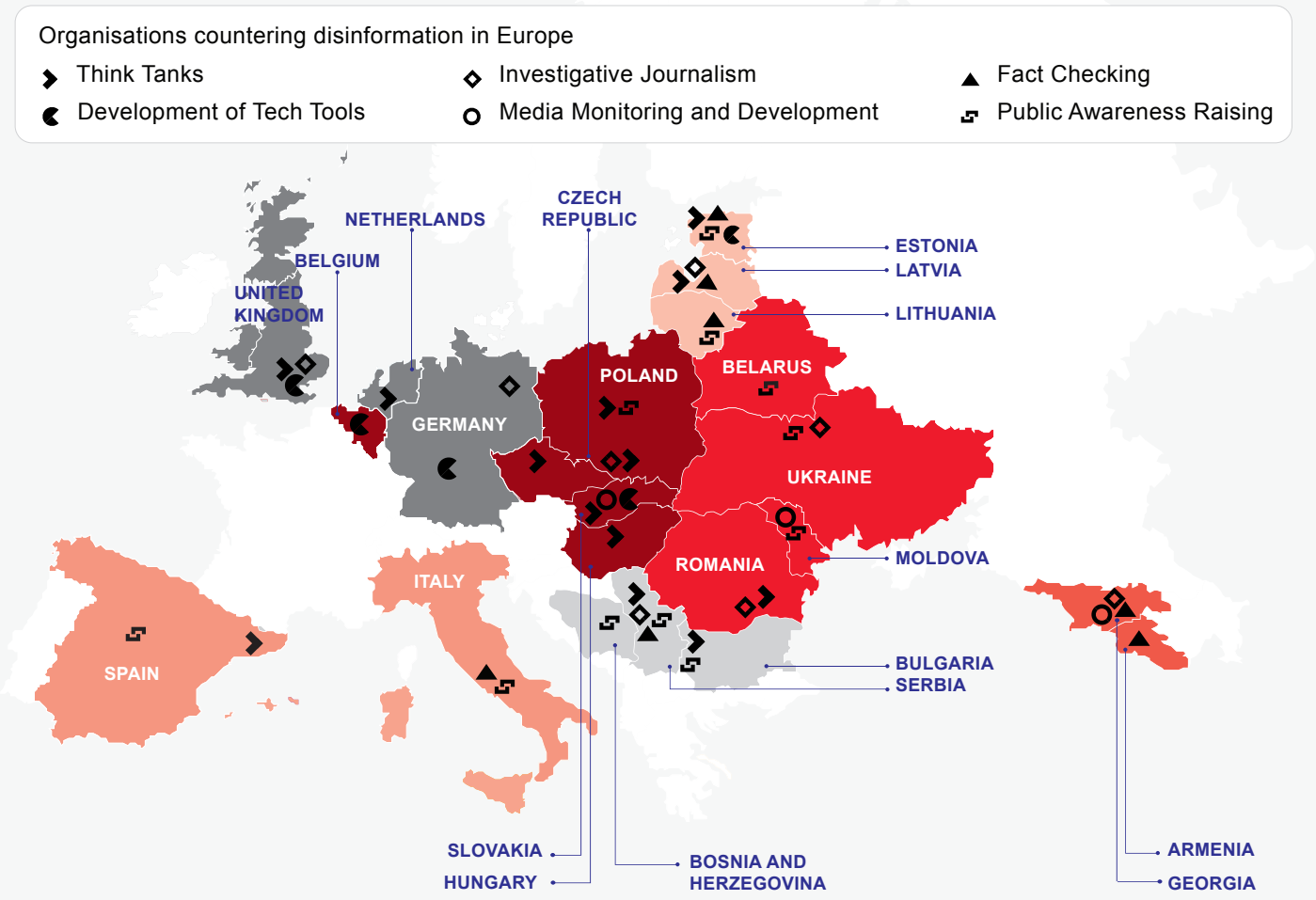


Figure 2: A map of organisations countering disinformation in Europe, broken down by primary activity and organisation type.

BALTICS:

• International Centre for Defence and Security	Estonia
• National Centre for Defence and Security Awareness	Estonia
• Centre for East European Policy Studies	Latvia
• Latvian Elves	Latvia
• NATO Strategic Communications Centre of Excellence	Latvia
• Re:Baltica	Latvia
• Lithuanian Elves	Lithuania
• Delfi	Lithuania
• Laisves TV	Lithuania

BALKANS:

• Why Not	Bosnia
• Bulgaria Analytica	Bulgaria
• Center for the Study of Democracy	Bulgaria
• HSSF Foundation	Bulgaria
• Center for Euro-Atlantic Studies	Serbia
• European Western Balkans	Serbia
• Istinomer	Serbia
• Krik	Serbia

STRATEGIC APPROACH

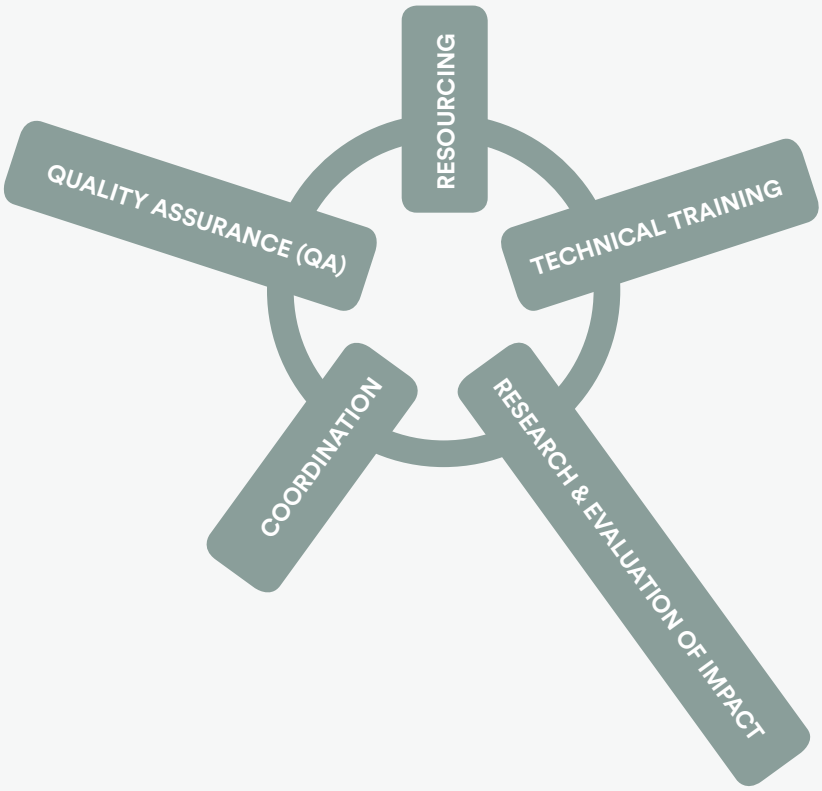
We recommend that these organisations above be invited to participate in the EXPOSE Network, ensuring a broad geographical reach as well as the potential to engage with many cross-cutting issues and to adopt a variety of tactics.

CENTRAL EUROPE:	
• European Values	Czech Republic
• The Prague Security Studies Institute	Czech Republic
• Political Capital	Hungary
• Center for European Policy Analysis	Poland
• Center for International Relations	Poland
• Centre for Propaganda and Disinformation Analysis	Poland
• Kosciuszko Institute	Poland
• Defence 24	Poland
• Fundacja Reporterów	Poland
• Institute of Public Affairs	Poland
• Warsaw Institute	Poland
• GLOBSEC Policy Institute	Slovakia
• Institute for Public Affairs	Slovakia
• IRI Beacon Project	Slovakia and Belgium
• Memo 98	Slovakia
• Slovak Security Policy Institute	Slovakia
CAUCASUS:	
• Sut.am	Armenia
• Coda Story	Georgia
• GRASS FactCheck	Georgia
• Media Development Foundation	Georgia
EASTERN EUROPE:	
• Euroradio	Belarus
• Association of Independent Press	Moldova
• Newsmaker	Moldova
• ZDG	Moldova
• Global Focus	Romania
• RISE Project	Romania
• Detektor Media	Ukraine
• StopFake	Ukraine
SOUTHERN EUROPE:	
• Fanpage.it	Italy
• Pagella Politica	Italy
• CIDOB	Spain
• Maldito Bulo	Spain
WESTERN EUROPE:	
• Correctiv	Germany
• Cicero Foundation	Netherlands
• Bellingcat	U.K.
• Factmata	U.K.
• Institute for Strategic Dialogue	U.K.
INTERNATIONAL:	
• DFRLab	
• Organised Crime and Corruption Reporting Project	

4.6 NETWORK ACTIVITIES

The Network Facilitator will deliver five core activity strands. These will run in parallel throughout the three-year implementation period. Resourcing will include a grant funding mechanism, and will ensure that organisations have access to legal, security and other operations support to enable them to deliver their work within a safe and well-resourced environment. Training will include a variety of learning packages, from online courses to embedded learning with dedicated specialists and regional events focused on topics including cyber security and enhancing communications outputs. The Quality Assurance (QA) strand will ensure that wherever possible outputs from Network members are created within rigorous journalism, fact-checking and legal frameworks and will drive to increase quality in both research and communications. Coordination of activities and network members will foster synergies between research interests, promote regional cooperation, and will facilitate networking, as well as drawing together activities and promoting specific approaches if necessary. Research and evaluation of impact will involve both a study of disinformation as it emerges online and the evaluation of the activities of network members to better understand their impact on the target audiences.

Figure 3: The Network Facilitator's five core activity strands.



4.6.1 RESOURCING

A) GRANTS MECHANISM

In addition to support and training, the Network will run a small grants mechanism programme for network members. This will ensure that smaller organisations without the capacity or ability to apply for large grants can receive funding in a quick turnaround cycle for smaller discreet activities that can otherwise be hard to fund.

Project Grants

Given the current spread of activity among potential network members and the gaps that exist, we recommend that grants should be awarded based on the following objectives:

- Improve coordinated research outputs into disinformation and its impact
- Increase public resilience to disinformation among vulnerable audiences

Seed Funding

We also recommend that grants be given to cover core funding over longer periods of time for smaller organisations, providing a guaranteed income that enables them to upscale and focus on delivery. There are a number of potential project partners whose work would be substantially enhanced if they had seed funding that freed up the founding members to deliver work rather than run day-to-day operations and fundraise. To receive these awards organisations would have to provide a three-year business projection of income and activities.

Applicants

These grants would work best when granted only to members of the EXPOSE Network. Members of the network will have already undergone vetting, entered into memorandums of understanding with the Network Facilitator, and complied with basic security guidelines while committing to developing more rigorous procedures.

Organisational Structure and Governance

Applications will be assessed by a Steering Committee, comprised of between eight and ten individuals representing larger organisations with a strong track record countering disinformation such as DFR Lab and the Atlantic Council, experts in delivering behaviour change campaigns and experts in research. These individuals should be representative of at least four different countries across Europe. This Steering Committee will be managed by the Network Facilitator.

B) LEGAL ADVICE AND SUPPORT

The network facilitator will offer a comprehensive legal support function, able to provide organisations with guidance on copyright, data protection and GDPR, and corruption and bribery. Alongside training, detailed later in the report, this would include ring-fenced days of legal support for a legal consultant to advise each organisation on their most pressing challenges, and pulling together a specific list of recommendations tailored to each organisation.

We also recommend ongoing support in the way of a dedicated email address for members to send their legal enquiries to, which can be prioritised by the Network Facilitator so that members can be signposted to the right support.

This will ensure that members are equipped to maintain high standards of integrity and compliance with international statutes, reducing their risk and increasing their long-term sustainability, and protecting their reputation and thus the reputation of efforts to counter disinformation Europe-wide. This will in turn protect the reputation of the FCO and other donor communities.

C) SECURITY SUPPORT

The network will offer ongoing security support including hosting a secure communications and information sharing network (See ANNEX C: Information Sharing Protocol). Members will be required to sign up to a basic code of conduct regarding cyber security, with milestones established throughout the three years of the programme duration that will take them to a higher level. These minimum guidelines will include:

- Device protocol; limit the access of data to personal devices. Ensure that all devices that can access network information are either centrally-managed by network members, or that they have to be approved and whitelisted by senior members of staff at member organisations.
- A cyber threat management and reporting function; members will be responsible for reporting cyber threats to the Network Facilitator and to using software to tracks threats as they emerge.
- Staff vetting; provide a basic framework that network members must use when initially screening applicants for jobs in order to vet whether candidates could expose the network to any potential threats.
- Physical security; in specific countries standards for physical security would be laid out to include personal security and the security of buildings.

In addition, the Network Facilitator would provide:

- Continued risk assessment and analysis: this would inform a periodic security briefing but can also be used to brief partners of imminent issues or areas of weakness
- Periodic security briefing by geography
- Physical infrastructure security survey on a request basis or where partners are high risk
- Independent verification of source networks or individuals on request

4.6.2 TECHNICAL TRAINING

Training must be a core component of the Network. Access to high quality, free training is limited and in some cases impossible for organisations operating in high risk environments. Furthermore, the niche activities that network members are engaged in require specialist training that is hard to access.

We envision five barriers to learning:

- Size of organisations; the majority of the organisations surveyed are small, with teams of less than ten full-time staff, and without dedicated staff building up a strong skill set in one area. They must be encouraged and supported to upscale in order to ensure learning is spread evenly and that skill sets have the opportunity to deepen.
- Time pressure; organisations working to counter disinformation are operating in a fast-moving and pressured environment with a need to respond rapidly. Coupled with a lack of resources, this can result in a de-prioritisation of learning.
- Lack of resources; training must be accompanied with access to the right tools and software in order to ensure that learning can be capitalised on and translate to measurable outputs.
- Complex political and social environments; network members are operating in different political and social environments. Those in 'dual threat' environments may attempt to upskill while also facing governmental pressure and combatting extreme propagandist content. These present challenges to learning due to the restrictions placed on these organisations as well as the time pressures they face, and require a flexible and tailored learning approach.
- Skill disparity; while some organisations in the Network are operating at scale and have developed deep skill sets in specific areas such as fact-checking or investigative journalism, others require introductory-level training in a number of areas.

In order to address these barriers, the training offered by the Network Facilitator must be:

- Flexible; taking into account that many organisations face significant time pressure and need to spread out training alongside other activities and commitments.
- Tailored to context; aware that each organisation operates in a different environment and that approaches to research, legal and security concerns will vary.
- Easily accessible; tailored to the learning mechanisms that organisations regularly use and made engaging for learners of different levels.
- Peer-to-peer based where possible; utilising the skills of the more established members of the network in order to spread knowledge regionally and foster closer cooperation.
- Integrated within a resourcing structure; tied to the provision of specific tools, e.g. social listening training to be accompanied by the licensing of social monitoring tools for use by network members.

Training topics can be selected from the four learning areas previously identified: **research, communications, sustainability and operational functioning.**

D) RESEARCH

Training modules and programmes to enhance research skills should cover:

- Investigative journalism; developing the ability of Network members to use open source tools to identify specific disinformation narratives, particularly in response to events. There are a number of partners in the network who could deliver training in this stream.
- Journalism standards; developing awareness of the NUJ Code of Conduct, National Code of Conduct, and Poynter's Fact-Checking Code of Principles along with giving practical advice on how to implement these.
- Social media monitoring; provide training and tools to track Kremlin disinformation and responses online, as well as gauging the impact of counter narratives.
- Open source research; not only training but building the capacity of organisations to conduct digital investigations using open source approaches that can support both their investigative journalism and fact-checking activities. These skills could include, for example, geolocation of images and films, identification of deep fakes, and time coding and sequencing to establish lines of causation.

E) COMMUNICATIONS

Training modules and programmes to enhance communications skills should include:

- Behavioural science driven campaign development; train network members on how to target vulnerable audiences in their communications by identifying formats, messengers, and mediums that will resonate with their target audiences.
- Content creation; supporting network members to turn their outputs into engaging content, both digital and offline that is tailored to their audience's needs. This could include, for example, commissioning social video, press engagement, or partnering with broadcast TV and radio
- Digital promotion and targeting; supporting Network members to identify their audiences online through segmentation and analysis, use social media promotion (paid and organic) to ensure content is reaching their intended target audience, and use analytics and comment coding to iteratively optimise their content and dissemination.
- Event planning workshops; provide network members with the capacity and knowledge to plan and run events that further their objectives, addressing the lack of counter-disinformation activities occurring offline.
- Brand building; provide training on how to build online and offline brand engagement that will increase their audience share as well as positioning them credibly to vulnerable audiences.
- Design; provide Network members with the ability to use a full range of design software to create compelling content to share on social media channels, and to condense complex reports into easily shareable infographics.

F) SUSTAINABILITY

Training modules designed to increase the sustainability of network members should include:

- Grant proposal training; offer network members training on how to look for grant opportunities and how to write a successful application.
- Budget design; training on how to design budgets for a variety of potential donors
- Business planning; bespoke modules for different types of operation model, helping organisations to plan for future activities and to think about new types of income generation

G) OPERATIONAL SUPPORT: LEGAL AND SECURITY

Alongside a significant resource component supporting organisations with legal and security compliance, a training component should include:

- EU media law; provide training sessions in order to ensure that network members comply with EU law when reporting. This should minimize their risk of being sued and limit the potential loss of credibility associated with having to retract stories
- EU employment law; provide training to all network members to ensure that they understand their duties under the Equality Act 2010 and that they have the ability to adhere to it
- Bribery and anti-corruption training; work with network members to establish an anti-corruption and anti-bribery policy that all members will comply with
- GDPR; train all staff at network member organisations on how to comply with data protection legislation
- Risk management; training on how to design a risk management framework
- Cyber security; training on protecting organisations online

4.6.3 RESEARCH AND EVALUATION OF IMPACT

One of the largest gaps that was identified throughout the research was a lack of ability to define, evaluate and communicate impact. Few organisations working in this space have a clear understanding of the impact of Kremlin disinformation, the impact they are looking to achieve themselves, and a framework in place to measure this. This therefore remains an important component of the work of the Network Facilitator.

SOCIAL LISTENING AND MEDIA MONITORING

The Network Facilitator will provide a centralised social listening function and media monitoring, tracking key disinformation narratives across Europe and providing network members with up-to-date information about which narratives are being promoted and shared, how they are being spread, and their impact with specific audience segments.

In turn, organisations will be provided with access to the latest social listening tools and training in how to use them, building up regional expertise in monitoring disinformation and its impact on audiences. Over the three-year period, key organisations would be upskilled in social listening in order to gradually transfer responsibility to regional partners.

This will ensure that organisations are equipped with the knowledge and skills to identify, monitor and counter live disinformation narratives, including mapping the sources and networks of these narratives and the audiences that are the most vulnerable to them. This information can then be shared with the FCO, via the Network Facilitator, ensuring that all data is gathered with high contextual and linguistic capability and that skills are kept in the region.

SUPPORT MEASURING AUDIENCE IMPACT OF KREMLIN DISINFORMATION AND RESPONSES

The Network Facilitator will provide bespoke training, support and consultancy to Network members to help them engage critically with the effectiveness of both Kremlin disinformation and their own work, how they define this, how they measure it, and how they communicate this to outsiders, be they policy makers, funders or peers.

This will ensure that organisations are able to effectively evaluate the impact of both Kremlin campaigns and their activities to counter and debunk disinformation, as well as to measure their effectiveness compared to the activities implemented by other organisations. This data will further help the FCO and the Network Facilitator to ensure support is channelled in the most effective manner, and will provide a comprehensive picture of which activities are the most effective in shifting public opinion and building resilience to disinformation.

4.6.4. COORDINATION

There is a huge amount of talent, commitment, and high-quality activity taking place across Europe by civil society organisations. These activities need coordinating to ensure a more significant impact and to enhance information sharing and best practice. Where network members require capabilities offered by other organisations, the Network Facilitator will facilitate the sharing of resources and incentives for doing so. The Network Facilitator will also play a key role in translating and distributing research across borders to key stakeholders, ensuring that all relevant parties are aware of ongoing activity.

Specific research activities or communications outputs could be coordinated by the Network Facilitator, who would also organise networking events regionally and according to tactics implemented.

4.6.5 QUALITY ASSURANCE (QA)

The Network Facilitator will ensure that organisations are reaching the right audiences through the most relevant media with the right messages; raising awareness of disinformation in their countries and abroad, exposing the networks and sources that propagate false narratives, providing alternative narratives through high-quality content, developing public resilience to disinformation and ensuring policy makers and governments are equipped with the latest research.

They will ensure that research products follow rigorous methodologies, and that communications outputs, whether to policy makers, governments, journalists, or the general public, are to a high standard and reaching the audiences they are intended for. The Network Hub will provide members with expertise in digital marketing, tailored to each organisation's different target audiences. This expertise could include help with online audience segmentation and targeting, developing brand identities and toolkits, support with developing PR packages, and training in low-resource filmmaking.

In delivering activities across the five strands of resourcing, training, QA, coordination of activities, and research and evaluation of impact, the Network Facilitator will achieve a joined-up approach that matches technical training with the provision of funds and tools, ensures activities are not only delivered to a high standard but coordinated in order to achieve maximum impact, and provides a crucial layer of impact measurement to all the work undertaken by Network members.

5. RECOMMENDATIONS

5.1 OVERVIEW

This project aims to counter the impact of Kremlin disinformation campaigns across Europe, increase awareness of and understanding of the issue and build societal resilience in the long term.

The FCO is seeking a service provider to operate as a Network Facilitator for the EXPOSE Network. This will involve the resourcing, training and coordination of civil society organisations and media outlets across Europe who are countering disinformation, alongside the measurement of impact through research and evaluation, and acting as a quality assurance mechanism for all outputs.

The expected impact of the programme is that a wider number of stakeholders across Europe including the greater public, media outlets and journalists, governments and policy makers, will become better informed about Kremlin disinformation and more resilient to it thus reducing its impact on society. The project intends to achieve this impact through the outcome of the strengthened capacity of civil society organisations around Europe to conduct research and deliver communications exposing disinformation.

5.2 BACKGROUND

There is a pressing need to counter disinformation with high quality, credible content that exposes and counters false narratives in real time and builds resilience over the long-term among populations vulnerable to Kremlin attack. The complexity of Kremlin-backed disinformation and its regional nuances require a response that is regionally based and adaptive to local scenarios, but also draws on a broader understanding of the Kremlin's strategic goals. A response must therefore have within its grasp a full range of tactics to be implemented at different times and in multiple contexts in response to an emerging and rapidly shifting threat.

Due to the scale and gravity of the threat across Europe, there are an increasing number of organisations with a high commitment to understanding and countering Kremlin-backed disinformation, often doing so in the face of strong opposition and with little remuneration or support for their work.

These organisations include civil society organisations, think-tanks, technology companies, media outlets, and grassroots implementors running projects that range from fact-checking to promoting media literacy or community cohesion. However, these organisations have limited operational capacity to do this work at the pace and scale required. Even within countries, they are often operating in isolation leading to duplication, gaps in delivery and little sharing of best practice. Their outputs are of varying degrees of quality and effectiveness, are not informed by the latest data and research, and are not tailored to their audience's needs.

Research suggests that organisations require improvement in four key areas to enhance the quality, pace and scale of their work:

- **Research** including social media listening, digital analytics, and open source research
- **Communications** including communications planning, content production and campaign delivery
- **Sustainability** including funding
- **Operational functioning** in areas such legal, data and security protocol

The model of EXPOSE Network sets out to bring together organisations in such a way as to effectively address these gaps and weaknesses. It is anticipated that this Network will operate with between 50-60 members who comprise of think tanks, media outlets, investigative journalism hubs, and grassroots implementors. While the majority of these have been pre-identified including undergoing rigorous due diligence checks and pre-selection interviews, there will be scope to add additional members if required. The Network Facilitator will be responsible for onboarding these members into the network.

An opportunity exists to upskill civil society organisations around Europe in these areas, enhancing their existing activities and unleashing their potential to effectively counter disinformation. If supported to deliver their activities in a professional manner that holds them above reproach, while gaining access to a variety of support functions, best practice and high-quality training, these organisations have the potential to be the next generation of activists in the fight against Kremlin disinformation.

5.3 THEORY OF CHANGE

IF a centralised hub is established and overseen by a Network Facilitator which resources Network members through the provision of grant funding, legal and security support, they will receive technical training, they will be better able to research and evaluate the impact of disinformation and counter-disinformation activities, their activities will be linked up with others in the region drawing on best practice, and they will have access to a quality assurance mechanism

THEN

- Network members will have increased capacity to deliver counter-disinformation activities
- Their activities will be informed by research and data and targeted at specific audiences
- Knowledge will be shared amongst network members
- Synergies will be identified and gaps and duplication addressed

THEREBY

- Increasing the quality and quantity of counter-disinformation content
- Increasing the sustainability and professionalism of organisations countering disinformation
- Creating an ecosystem of credible voices which can continue to grow and counter the disinformation ecosystem exploited by the Kremlin
- Building awareness amongst key audiences including policy makers, journalists, the general public, and influencers/amplifiers of Kremlin strategy, tactics and networks
- Helping to establish best practice on countering disinformation

CONTRIBUTING TO

- Undermining the credibility and effectiveness of Kremlin disinformation campaigns
- Building resilience to disinformation in vulnerable and mainstream audiences across Europe
- Increasing awareness of Kremlin disinformation among governments, policy makers, the media, online amplifiers and the general public.

5.4 SCOPE

The Network Facilitator will deliver five core activity strands. These will run in parallel throughout the three-year implementation period.

- **Resourcing** will include a grant funding mechanism, and will ensure that organisations have access to legal, security and other operations support to enable them to deliver their work within a safe and well-resourced environment.
- **Training** will include a variety of learning packages, from online courses to embedded learning with dedicated specialists and regional events focused on topics including cyber security and enhancing communications outputs.
- **Research and evaluation of impact** will involve both a study of disinformation as it emerges online and the evaluation of the activities of network members to better understand their impact on the target audiences.
- **Coordination** of activities and network members will foster synergies between research interests, promote regional cooperation, and will facilitate networking, as well as drawing together activities and promoting specific approaches if necessary.
- The **Quality Assurance (QA)** strand will ensure that wherever possible outputs from Network members are created within rigorous journalism, fact-checking and legal frameworks and will drive to increase quality in both research and communications.

RECOMMENDATIONS

Component One:
The resourcing of organisations through grant funding and legal and security support

- Grants mechanism
- Legal advice and support
- Risk Management and security support
- Information Sharing Protocol

Component Two:
The provision of technical training

- Online Technical Training
- Offline Technical Training
- Embedded Learning
- Access to software

Component Three:
Establishment of a unit for research and evaluation of impact

- Social listening and media monitoring
- Research and evaluation

Component Four:
The coordination of activities

- Translation and distribution of research across borders
- Networking events
- Coordination of public facing campaigns
- Coordination of research activities

Component Five:
A quality assurance mechanism

- Digital communications support
- Research support

In delivering activities across the five strands of resourcing, training, QA, coordination of activities, and research and evaluation of impact, the Network Facilitator will achieve a joined-up approach that matches technical training with the provision of funds and tools, ensures activities are not only delivered to a high standard but coordinated in order to achieve maximum impact, and provides a crucial layer of impact measurement to all the work undertaken by Network members.

RECOMMENDATIONS

FUNDING

Table 2: Estimate of Funding = £3,000,000 per year

ACTIVITY	YEAR 1	YEAR 2	YEAR 3
COMPONENT ONE: RESOURCING	**50%**	**45%**	**45%**
Grants mechanism (estimated 30% per annum)			
Legal advice and support			
Risk Management and security support			
Information Sharing Protocol			
COMPONENT TWO: TRAINING	**20%**	**15%**	**15%**
Online Technical Training			
Offline Technical Training			
Embedded Learning			
Access to software			
COMPONENT THREE: RESEARCH AND EVALUATION UNIT	**14%**	**14%**	**14%**
Social listening and media monitoring			
Research and evaluation			
COMPONENT FOUR: COORDINATION OF ACTIVITIES	**8%**	**16%**	**16%**
Translation and distribution of research across borders			
Networking events			
Coordination of public facing campaigns			
Coordination of research activities			
COMPONENT FIVE: QA MECHANISM	**8%**	**10%**	**10%**
Digital communications support			
Research support			

RECOMMENDATIONS

GOVERNANCE AND REPORTING

The Network Facilitator will report to the FCO monthly on progress, and will establish a reporting mechanism for live data to be shared from the Research and Evaluation unit to the FCO monitoring disinformation in real time and the impact of the efforts of Network members to counter it.

A steering committee will be established by the Network Facilitator to assess grant applications, comprised of between 8-10 individuals representing larger organisations with a strong track-record of countering disinformation, experts in delivering behaviour change campaigns and experts in research. These individuals should be representative of at least four different countries across Europe.

SECURITY

The implementer will hold the duty of care responsibility for its staff and the security of the project; it is to ensure that all reasonable security measures (physical, information and communication) are taken to reduce the threat to as low as is reasonably possible, and to expose any risks that are identified.

The Network Facilitator will be responsible for setting up an Information Sharing Protocol for secure network correspondence. This has already been designed and tested.

Upskilling to Upscale:

Annexes

ANNEX A: NEEDS ASSESSMENT FINDINGS

ANNEX B: RISK MANAGEMENT FRAMEWORK

ANNEX C: INFORMATION SHARING PROTOCOL

ANNEX D: PROPOSED NETWORK MEMBERS

ANNEX E: REGIONAL REPORTS

Upskilling to Upscale:

Annex A

NEEDS ASSESSMENT FINDINGS

ANNEX A: NEEDS ASSESSMENT FINDINGS

1 LEGAL COMPLIANCE AND UNDERSTANDING

1.1 WEAKNESSES IDENTIFIED

Over 80% of respondents have no anti-bribery and anti-corruption policy or code of conduct in place and uncodified procedures seemingly only in place with respect to hospitality. Regardless of the size, structure or market of the organisation, top level management commitment to bribery and corruption prevention should include, as a minimum, (1) communication of the organisation's anti-bribery and anti-corruption stance, which can be achieved by way of a policy or code, and (2) an appropriate degree of involvement in developing bribery and corruption prevention procedures. Those procedures should be communicated internally and externally to demonstrate an organisation's zero tolerance approach.

Only 5% of the respondents provide basic training on legal compliance. That, combined with a lack of internal procedures to prevent bribery and corruption, means that there is likely to be a deficiency in employee skills and knowledge. Communication and training can deter bribery and corruption by enhancing awareness and understanding of a commercial organisation's procedures and to the organisation's commitment to their proper application.

A small percentage of respondents had faced an allegation of bribery or corruption but there was disparity across all respondents as to how an allegation would be dealt with in practice. Perceived appropriate responses ranged from 'informing the police' to 'expulsion' and third party 'audit[ing]'.

More than 80% of respondents do not have a written discrimination policy that is communicated to staff. While a less formal approach may be considered sufficient, organisations are more likely to be able to comply with their duties under the Equality Act 2010 and prevent their employees from discrimination if they establish a policy to ensure equality of access to their services from all groups of society.

Despite the forthcoming changes being introduced by the GDPR, less than half of the respondents have trained their team to understand data protection principles. The organisations identified need to be made aware of the GDPR, its extra-territorial scope and the sanctions and remedies that may be enforced for non-compliance.

1.1.1 BARRIERS TO LEARNING

The broad extra-territorial application of the Bribery Act 2010 means that bribery outside of the UK can attract the attention of authorities in multiple jurisdictions. The various guidance broadly suggests the sharing of information and consultation between jurisdictions so that the agency best able to deal with the matter leads the investigation and prosecution. In practice however, matters are not so straightforward; educating overseas organisations about the scope of the legislation and helping them to interpret and understand the implications is challenging.

An investigation, prosecution or settlement for a Bribery Act related matter with either the Serious Fraud Office or the Crown Prosecution Service does not preclude any other body from investigating the same matter and taking enforcement action where permitted under the laws of that jurisdiction.

ANNEX A: NEEDS ASSESSMENT FINDINGS

1.1.2 LONG TERM RESOURCING REQUIREMENTS

The provision of anti-discrimination training to staff, including those not providing a direct service to the public, and embedding a discrimination policy requires resource and in smaller organisations this may lead to its implementation being overlooked.

Educating organisations about the GDPR and its extra-territorial scope, getting that message across to organisations in an easy to understand manner, and translation of that material as appropriate, is crucial.

The top-level management of those organisations could consider (1) identifying someone of a suitable level of seniority to be a point of contact for queries and issues relating to bribery risks, (2) the selection and training of senior management to lead anti-bribery and anti-corruption training amongst their direct reports and (3) an internal launch of an anti-bribery and anti-corruption policy and code of conduct with a message of commitment to from senior management.

A greater number of respondents stated that they incorporated anti-bribery and anti-corruption clauses into contracts and conduct some form of basic due diligence check. While this suggests that they are aware of the commercial risks and seek to protect the organisations from bribery committed by third parties, the language of those clauses and the manner in which due diligence is conducted could be strengthened by making available (1) boilerplate anti-bribery and anti-corruption clauses in clear easy to understand language free from legal jargon, and (2) an online due diligence ('know your client/supplier') checker, both free at the point of access.

1.1.3 TOOLS AND SUGGESTED FRAMEWORK

The drawing up of a checklist for non-UK organisations to take steps to comply with GDPR and cross-border transfer restrictions should be considered. This should (1) identify specific countries, territories or international organisations outside of the EEA where the organisation may transfer data, (2) determine whether the data recipients outside of the EEA need to make any onward transfers, (3) identify whether the recipient country provides adequate privacy protections under the GDPR, (4) document the basis for the cross-border transfer for evidentiary purposes.

Moreover, to ensure that member organisations are equipped to maintain high standards of integrity and compliance with international statutes, corruption and bribery laws, and data protection, the Network Facilitator should provide: (1) ringfenced days of legal advice; (2) training in compliance; (3) legal surgery with an EU media lawyer.

ANNEX A: NEEDS ASSESSMENT FINDINGS

2 ETHICAL JOURNALISM STANDARDS

2.1 INTRODUCTION

The Network encompasses several distinct geographical areas, each of which differ in key respects. This means that the Network as a whole is uneven and the organisations examined within it are subject to varying financial, political and security considerations that affect – at times greatly – their individual capacity and freedom to work in the space. The influence that their work has is accordingly also affected.

This report assesses the envisaged Network organisations according to the ethical journalism standards they adhere to. This is a vital area across the Network as a repeated refrain from almost all organisations interviewed was the that "the answer to fake news is quality news." Put more simply: high quality journalism is a vital means of contesting disinformation.

This is especially true of organisations within what is termed 'dual threat" countries, where organisations are battling not just Russian disinformation but hostile/pro-Russian governments. These environments often also overlap with the most resource-poor states, such as Moldova, where the NGO sector is almost non-existent and those at the forefront of battling Russian propaganda are independent newspaper outlets.

Ethical journalism standards are assessed according to four key criteria: (1) weaknesses identified; (2) barriers to learning; (3) long-term resourcing requirements; (4) training tools and suggested framework.

2.2 WEAKNESSES IDENTIFIED

There is a clear lack of official adherence to the NUJ Code of Conduct and National Code of Conduct. There is also limited knowledge of the Poynter International Fact-Checking Code of Principles. Although there are some exceptions, many organisations do not implement these codes or principles, even if similar measures are enacted.

In countries that are (1) on the frontline of Russian disinformation campaigns, and (2) have governments that are aware of the threat and seek to combat it, adherence to, and knowledge of, the aforementioned codes and principles was greatest. This was particularly evident in the Baltic States, Poland and Ukraine. However, even here, best practice is generally determined by what is repeatedly described as "Western standards" of journalism and what they consider to be common sense.

In the Baltic States, organisations generally adhere to ethical standards involving rigorous checking with multi-source confirmation and tracking the footprint of information. The standards mentioned above are not in themselves always adhered to but are met through local best practice. For example, volunteers on social media who call themselves the 'Lithuanian Elves' identify disinformation on social networks, fact-check the misleading statements and comments, and report them if they are in violation of social networks' community rules.

In Poland, organisations like Fundacja Reporterów, again adhere to traditional journalistic best practise and have an awareness that different countries have differing media and libel laws.

In dual-threat countries, knowledge of the above standards is weakest. In particular, knowledge of the Poynter Fact-Checking Code is limited, with even outfits of high capacity like Bulgaria's Center for the Study of Democracy unaware of it. Again, however, organisations focus on best practise in all their output.

Even in resource-scarce and dual-threat countries like Moldova and Belarus there is a de facto attitude of not trusting anything, whether it is an image or story, until it has been independently verified. Investigative journalistic outlets like ZDG and Euroradio have what they refer to as Western standards of reporting. When pressed, however, the term seems a value judgement rather than adherence to a set criteria, with respondents either giving vague answers about "objectivity" and "balance" or saying they meant following standards set by blue-chip legacy media like the Guardian or New York Times. However, adherence to the NUJ Code of Conduct and knowledge of the International Fact-Checking Network Code of Principles is almost entirely absent.

Even in Southern Europe, where the field of journalism is more developed, the reporters of Maldito Bulo, a Spanish journalistic project with rigorous standards of journalism, relied on volunteers to fact-check each other's output rather than officially adhering to the NUJ Code of Conduct. Unlike most organisations interviewed they are aware of the Poynter Code of Principles. However, the belief running throughout the organisation, ranging from fact-checking to knowledge of libel laws, is that it is down to the individual journalist to be personally responsible. Given the high quality of the organisation's ouput, this method generally works well. However, it is very much conducted on an ad hoc basis as opposed to working around a unified set of principles (beyond the obvious, such as thoroughly checking sources).

Similarly, the Barcelona-based CIDOB did not adhere to any of the above principles but worked on a two-source confirmation principle, although it should be noted that it is a think tank, not a news organisation.

Ultimately, it is clear that organisations are insufficiently aware of the NUJ Code of Conduct and often totally unaware of the International Fact-Checking Network Code of Principles. Only Ukraine's StopFake actually found it "helpful as part of the broader holistic approach they believe is the key to success in this field." However, the organisations are performing competently, and almost none had been successfully sued.

2.3 BARRIERS TO LEARNING

Of all the organisations interviewed across the Network, and across all competencies discussed, the greatest barriers to learning are financial and human resource limitations. This is a near universal problem.

Another common problem is that many of the organisations interviewed are not journalistic publications but NGOs. As such, they often do not employ professional journalists but rely on their own researchers. However, entities like Hungary's Political Capital, which is highly competent, employ journalists on a project basis.

Across the board there was a request for greater capacity building in this area. Even strong journalistic publications working in dual-threat environments like Moldova's ZDF requested greater capacity in helping to identify disinformation.

If the Network is to get organisations to adhere to and officially implement the various methodologies then training and capacity are needed. Without these, significant barriers to learning remain.

2.4 LONG-TERM RESOURCING REQUIREMENTS

Again, the greatest need for almost all organisations is increased financial and human resources. Failing this, training and capacity-building are the means by which advances in this area will be made. Indeed, this area lends itself to more cost-effective means of improvement as almost all of the organisations involved are reasonably strong in this area. Organisations mainly just need development and improvement rather than, as in other areas, displaying a total lack of capacity that would need to be built from the ground up. There is great potential to upskill here with comparatively minimal cost.

2.5 TRAINING TOOLS AND SUGGESTED FRAMEWORK

Training and capacity building must be initiated at a pan-Network level. Different areas facing different threats will require different training. In the Baltic States and Ukraine, where organisations work with extremely supportive governments to battle Russian disinformation, training should focus on further developing a synergy between government and the Network organisations as this is the relationship best suited to combating Kremlin output.

In dual-threat countries, which often also suffer from greater resource scarcity, training should be tailored to adhering to the above standards while facing governmental pressure as well as combating propagandist content. At present the former hardly exists and this is a lacuna that must urgently be filled.

A goal of the envisaged Network is to increase ties between its constituent organisations and where possible organisations with greater capacity in the Network – like Ukraine's StopFake and the various Baltic organisations. These more capable organisations could offer training and capacity building to those that (1) exist in more challenging environments, and (2) face more challenging restraints.

A framework of peer-to-peer learning would thus provide for (1) a greater sharing of best practice and knowledge; and (2) ideally increase ties and cooperation between organisations in the Network. With possible additional assistance from the client as well, significant advances could be made in this area.

ANNEX A: NEEDS ASSESSMENT FINDINGS

3 SECURITY

3.1 WEAKNESSES IDENTIFIED

Based on our initial enquiries, organisational approach to risk management varies across the range of partners identified. Of the responses to our Cyber Security Questionnaire, the biggest weakness broadly identified is the subjectivity of risk management. Across partners, the methods for identifying risk vary widely, and the benchmarks for mitigating risk and implementing adequate cyber security measures differed considerably. Risks are identified and monitored in an ad hoc manner, relying on shared information, some software and some specialist support

3.1.1 INFORMATION SECURITY

When asked about information security policies, some partners had nothing in place, some relied on general awareness or basic training, and some claimed to be well informed and more specifically trained in the risks associated with their activities. Where they had information security policies or something similar, most partners reviewed these annually, but one partner reviewed them monthly.

Of those responsible for maintaining security policies, the individuals ranged from IT Manager to CEO. This would suggest different approaches to security and possibly gaps in provision, dependent on that individual's experience or perspective. For instance, a CEO is likely to approach from a business or financial outlook, whereas an IT Manager may have a more technical perspective. This is a weakness because of the potential lack of consistency across partners.

Resourcing is the clearest challenge to Information Security. Weaknesses were identified in the range of individuals responsible and the different approaches they may have to understanding risk and mitigating it. Some partners had various departments and parties responsible for

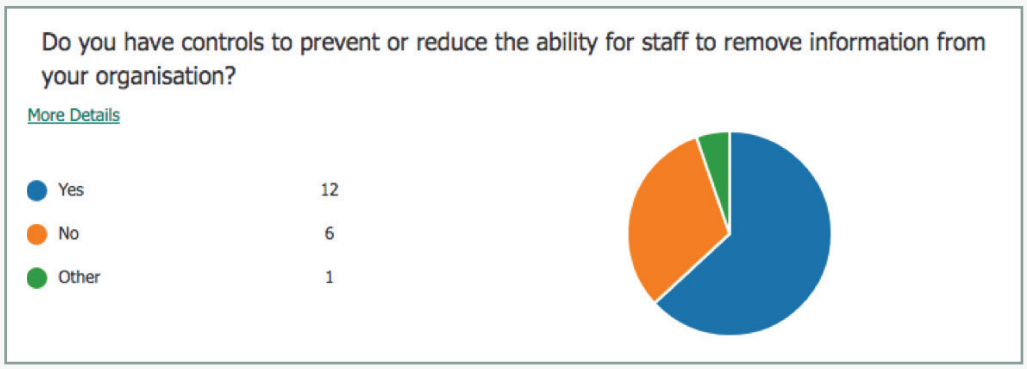
security, which could result in gaps in provision if one owner is not responsible across all aspects. It appears that an understanding of cyber security, physical and personal risks is inconsistent and varies widely across organisations.

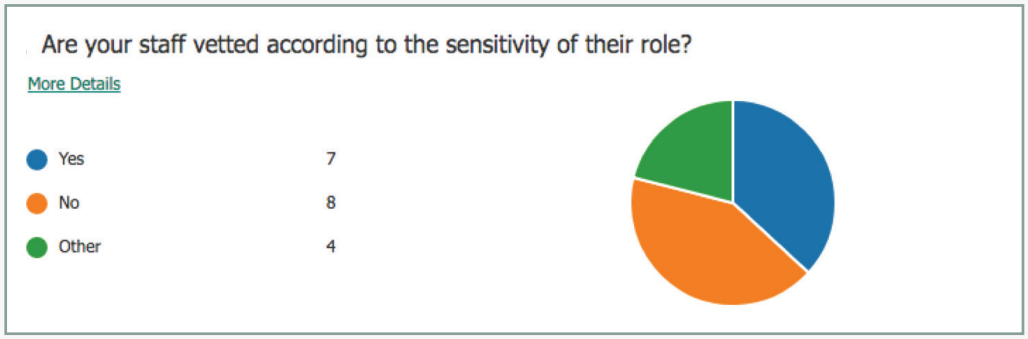
In the event of a security breach, some partners had no process in place to inform clients or funders, some were immediately required to disclose the breach and others took a case-by-case assessment to decide on their course of action. While working as part of a partnership, it is important that all organisations apply the same process to communicate a breach to clients and affected parties. It is advisable that a central policy is determined to manage these scenarios.

3.1.2 TECHNICAL SECURITY

This lack of consistency is apparent in the operation of hardware infrastructure and devices used within the organisations. The acquisition, maintenance and disposal of hardware occurs alongside an understanding that hard drives should be securely wiped or destroyed to prevent data leaks, for example. However, some partners operated a Bring Your Own Device (BYOD) policy or relied on staff maintaining their own equipment. BYOD comes with the inherent risk that these devices are not centrally managed and are thus far more susceptible to compromise.

If a device is compromised then it may be easier for a threat actor to access sensitive partner data. Across organisations, data is stored in a variety of cloud or on-site server locations and not all partners check the security of new systems before deploying them. There is a mixed approach to data encryption, data backup and the verification of the integrity of stored data. Many partners have no controls in place to restrict the ability of their staff to remove information and many of the same partners do not vet staff according to the sensitivity of their role.





ANNEX A: NEEDS ASSESSMENT FINDINGS

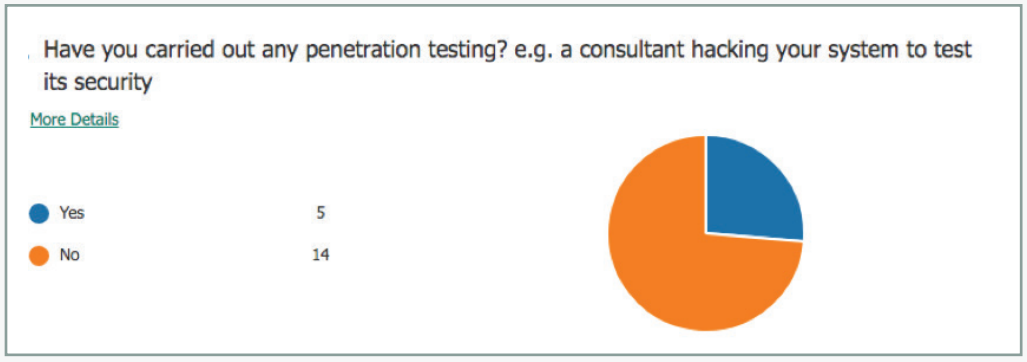
General physical office security seems to be understood and measures taken, but data security questions were less comprehensively answered suggesting that this has not been taken into consideration. Most partners had firewall protection on devices and servers, and in most cases the network is monitored for attacks to a limited extent.

Where partners operated a BYOD policy, there is a clear risk. Individuals using various devices at different security patches with little or no centralised management are open to a multitude of vulnerabilities which could then compromise their organisations. Storing data in numerous locations increases the risk of data leak, because there is no centralised control or audit trail. The fact that several partners claimed not to hold sensitive information raises concerns over an accepted definition of what constitutes sensitive data.

There is a human risk in several of the organisations given that staff are not vetted. Where due diligence is carried out on new staff, the provision of this ranges from secret level classification through to general social media background checks. Within organisations, there is an inconsistent approach to sharing access to files.

While many of the partners have basic network protections like firewalls in place, it is clear that not all have considered a disaster recovery process or tested this process in the event of a security incident like a cyber attack. Most organisations do not have a system to log, manage and review security incidents.

Most had not carried out penetration testing of their networks.



3.2 BARRIERS TO LEARNING

The size of the organisations is a clear barrier to applying rigorous security policies. Some of the partners identified are very small and have limited resources and experience. Applying blanket security across the board is likely to resisted, in the event that it changes established ways of working or applies more 'red tape' to activities. While the intention is not to deter flexibility or responsiveness, it should be acknowledged that security and flexibility are at different ends of the spectrum. A balanced approach will need to be taken to address specific partner environments.

3.3 LONG-TERM RESOURCING REQUIREMENTS

Resourcing requirements will differ across the range of partners. The organisations at the top end of this scale appear to have a relatively sophisticated approach to information security. Bringing the other partners up to this level is likely to require investment in their physical infrastructure, the provision of standard policies, and technical support to maintain their cyber capabilities in a secure way.

As well as a centralised security breach process, centralised risk management is advisable, given the ad hoc approach to identifying, assessing and mitigating risks. Partners could benefit from sharing information, but it would be sensible to funnel this through the Network Facilitator to verify and assess risk against set benchmarks. Information regarding these risks should also be shared through agreed communications protocols.

To mitigate the risk of compromised communications, the safest approach is to bring all partners onto the same communications platform. By implementing and enforcing a secure portal for sharing information, it is easier to apply a consistent approach to security. All communications should take place in the same agreed manner, with all data to be stored in the same secure location, and all sharing to take place using agreed, verified methods. It will require ongoing license subscription costs and centralised management costs to maintain a secure portal.

Where partners operate a BYOD policy, it is advisable to provide hardware that can be centrally managed, or at the very least submit devices for inspection and ensure they have up-to-date antivirus, malware and anti-ransomware protection. Partners should be supported in bringing their assets up to a secure standard or otherwise devices should be centrally provided and centrally managed to ensure consistency.

3.4 TRAINING TOOLS AND SUGGESTED FRAMEWORK

The biggest challenge to security across this framework is likely to be applying consistency. Partners will have established ways of working, and different communication methods. Where multiple methods are used, data will exist across multiple platforms, accessible by multiple parties. While this spreads the risk, it also increases the variety of vulnerabilities. The same applies where BYOD policies mean that many different types of hardware are used within an organisation.

A framework should be put in place to ensure partners receive consistent training and are aware of the risks faced. This training should include physical considerations, from the office environment to the hardware devices utilised. Staff should be made aware of the technical vulnerabilities associated with out-of-date software, through to the need to manage devices that have access to sensitive data.

This framework should include considerations for data storage, access control and information rights management, as well as the processes that should surround such measures. This framework could follow aspects of a global accreditation, such as IS27001 for information security, and could utilise aspects of a Government-approved standard such as Cyber Essentials Plus. A hybrid approach that is tailored towards our specific partners is recommended.

4 RESEARCH

4.1 INTRODUCTION

Research is at the heart of countering Russian disinformation because the battle involves both debunking content and exposing networks, as well as the ability to produce compelling counter-disinformation content. The key tactics identified as vital to best practice in this field are fact-checking, open source research and mapping propagandist networks.

4.2 WEAKNESSES IDENTIFIED

The greatest gap in the Network is fact-checking. Many organisations do not engage with it either because they believe there are enough dedicated fact-checking organisations in operation or because they doubt its efficacy.

One of the few large, multi-pronged organisations combating Russian disinformation, StopFake, began as a fact-checking organisation and will continue to focus primarily on fact-checking. Indeed, it is presently hiring more editors. Given the conflict between Ukraine and Russia, it considers its activities necessary for national security reasons. For example, StopFake's Russian partners recently fact-checked a major Russian documentary on Putin that was "filled with lies". StopFake immediately shared their findings and thus increased their visibility. But as a large institution it remains an outlier.

Organisations dedicated to fact-checking are strongest in the Baltics. For example, the Lithuanian portal Delfi, the largest fact-checker in the country, runs a debunking project called "Demaskuok" ("uncover"), which asks their readers to submit stories that they think might be inaccurate for Delfi journalists to fact-check.

A far greater weakness was the ability to monitor social media, especially in the Balkans, Central Europe and Eastern Europe. Of the organisations interviewed here not a single one was aware of online listening tools such as Brandwatch or Affinio.

ANNEX A: NEEDS ASSESSMENT FINDINGS

Almost all organisations interviewed expressed a desire for greater data science capabilities. Critically, an issue for many was not skills but resources. Bulgaria Analytica, for example, while expressing a strong interest in capacity here, also noted that Bulgaria has around 40,000 people writing software for US companies. The skill set is present, making it easy to train people in this area. The ground is fertile; only resources are lacking.

The capacity to conduct long-term research (or in-depth investigations in case of journalistic outlets) was present in most organisations, which produced reports with comparative regularity. Even those in dual-threat countries have capability in this area.

Sofia's HSSF Foundation, for example, engages in media monitoring. HSSF Foundation identifies pro-Russian talking points and measures the frequency with which they occur in the Bulgarian online media. They recently published an in-depth report examining the period 2013-2016 and are now working on a follow-up report looking at 2017. The reports are published on news websites and blogs and on their website. Similarly, Serbia's European Western Balkans has also engaged in several large research projects in this area.

There was also capacity to monitor propagandist networks, a vital function to combat disinformation, and far more effective than fact-checking. The Slovakian think tank the Institute for Public Affairs is strong in this area: it has mapped members of pro-Russian organisations influencing the public debate in Slovakia. The Czech Republic also boasts highly developed capabilities in network mapping in the form of organisations like the European Values Think-Tank, which also mapped corruption (which often goes hand in hand with disinformation). However, there were also gaps in the Network in this area. Georgia's GRASS, for example, was keen to enter the space but is at present forced to rely on work done by other experts in the field.

It is evident that the level of research capability is uneven across the organisations. The majority of organisations do not focus on fact-checking and almost all have severe weaknesses with regards to using data science and online listening tools. A high competence in the ability to produce research products was present throughout the Network, but again, with clear exceptions.

4.3 BARRIERS TO LEARNING

The greatest barriers to learning are financial and human resource limitations. This is a near universal problem. This is particularly acute in the area of research where, generally speaking, skills are not lacking but the resources to upskill are simply not sufficiently present to the requisite degree.

There is also a severe knowledge gap in the area of data science – this is almost universal – that amounts to a huge barrier to learning. This defect is critical to address. As information technology continues to advance so will the sophistication of Kremlin disinformation. Keeping up with the technology, and having the means to use it, is vital in the fight against propaganda.

Organisations in dual-threat countries also face domestic opposition and the envisaged Network is likely to face pushback from certain domestic governments and local actors.

ANNEX A: NEEDS ASSESSMENT FINDINGS

4.4 LONG-TERM RESOURCING REQUIREMENTS

Greater resources – both human and financial – are needed across the Network in almost all categories. But the focus must be on providing greater capacity in the fields of data science and online listening. With computing increasingly moving toward AI, as well as developments in fintech such as the emergence of blockchain technology, Kremlin propaganda is going to enter a new and more advanced stage. Debunking falsehood and producing written reports will no longer be sufficient (though they will of course retain their importance).

Whatever resources are available must be focused on these areas, especially AI and data science. Other areas can be upskilled through capacity building and training.

4.5 TRAINING TOOLS AND SUGGESTED FRAMEWORK

Training and capacity building must be initiated at a pan-Network level. Different areas facing different threats will require different training.

If an increase in fact-checking capability is needed, in terms of the development of research products, there is much to be said for peer-to-peer capacity building in this area. Organisations like Ukraine's StopFake and GLOBSEC's Stratcom initiative in Slovakia have much to offer partners with significantly less capacity and resources; they should therefore be encouraged to share best practice through forums, conference and tutorials (even online or via Skype if resources are stretched). As with all areas, this will have the additional benefit of bringing members of the Network into closer contact and increasing cooperation and the sharing of knowledge and skill sets.

The biggest gap remains data science capabilities. There are, however, clear opportunities for upskilling here, apart from mere capital injection, that can greatly increase capability across all areas. The biggest 'quick win' would be for the Network Facilitator to organise regional training hubs centred on leading organisations within the Network that would also provide some limited grant-giving capability to allow the relevant organisations to purchase appropriate software. This could also be done more centrally by the Network Facilitator. This must be addressed. It is this field that the next generation of disinformation will inhabit.

5 PUBLIC FACING COMMUNICATIONS

5.1 INTRODUCTION

Public communication is at the heart of any counter-disinformation effort. Without an ability to disseminate content, whether fact-checking, debunking disinformation, providing proactive counter-disinformation or exposing the networks that lie behind Kremlin disinformation, an organisation is rendered essentially ineffective in contesting the information space if they are unable to communicate their findings.

ANNEX A: NEEDS ASSESSMENT FINDINGS

It is in this area where the uneven nature of the Network is most pronounced. Those in single-threat environments, where organisations work in near concert with a supportive government, face a more conducive environment to getting their message across, even if it sometimes does not reach the most vulnerable audiences. Conversely, those operating in dual-threat environments, where they battle Kremlin disinformation as well as a hostile and/or pro-Russia government, face the largest obstacles to public-facing communications.

5.2 WEAKNESSES IDENTIFIED

There was a clear difference between single- and dual-threat countries identified. In Ukraine both StopFake and Detektor Media have few weaknesses in communicating to the public, supported as they are by extensive government apparatus.

It is instructive to note the difference between the regions. In Poland, the Kosciuszko Institute organises the annual CyberSec Forum, which brings together a wide variety of influencers to help build a Europe-wide cybersecurity system. They are keen to take on the role of a network convener and are interested in developing recommendations on how governments can build counter-measures and increase resilience to disinformation.

Meanwhile, Polish media outlet Defence24 is the biggest new portal on defence-related issues in Poland. They publish articles related to disinformation and information security that reach thousands of readers.

In Slovakia, which does face some government hostility, GLOBSEC are arguably the premier organisation in the space. The success of its outreach can be seen from one online campaign to illustrate the risks posed by disinformation in collaboration with two leading Slovakian bloggers, which achieved 1.2 million views in a country of GLOBSEC assessed it as the most successful counter-disinformation campaign in the region.

Meanwhile, in Moldova, both ZDF and the Association of Independent Press face considerable official hostility, with the head of ZDF repeatedly receiving death threats and general pressure to cease her journalistic activities. Nonetheless, the reach of the publication remains relatively wide, though its effects are limited given the political landscape.

Organisations in this space are forced to be creative to ensure that their counter-disinformation is seen and heard. For example, API gives Moldovan citizens the capacity to report fake news online or through an app. They have recently received a grant from the European Commission that will allow them to hire and train a network of 35 part-time staff across the country, comprising journalists and activists who enjoy credibility with local populations. The project started in April and will last for 20 months.

The weaknesses when attempting effective public communications in dual-threat countries are lack of resources and lack of co-ordination with local governments, which is often almost non-existent. All organisations also required greater social media monitoring and listening skills.

A

ANNEX A: NEEDS ASSESSMENT FINDINGS

5.3 BARRIERS TO LEARNING

Pro-Russia narratives here are often either subsumed within or subservient to broader anti-Western and anti-democratic narratives. These tend to focus on EU 'decadence', especially with regards to LGBT rights and lax borders, the atrophying of EU institutions, and the need for strong national leaders as opposed to faceless bureaucrats in Brussels.

Another barrier to combating disinformation is the fact that certain Kremlin-backed narratives are factually true. For example, the Serbian organisation European Western Balkans noted that one of the country's most prominent pro-Kremlin narratives relates to Russia's ongoing support for Belgrade in the Kosovo dispute, which is true. Responding to inconvenient truths, as opposed to pure propaganda, is naturally more problematic.

It is evident, then, that national political and social climates provide barriers to learning for organisations in various countries. At the organisational level the problems remain the same: lack of resources, especially in data science and social media. Capacity must be provided here.

5.4 LONG-TERM RESOURCING REQUIREMENTS

Greater resources, both human and financial, are, as above, needed across the Network in almost all categories. But the focus, again as above, must be on providing greater capacity in the fields of data science and online listening.

Whatever resources are available must be focused on these areas, especially AI and data science. Other areas can be upskilled through capacity building and training.

5.5 TRAINING TOOLS AND SUGGESTED FRAMEWORK

Training and capacity building must be initiated at a pan-Network level. Different areas facing different threats will require different training. Communication professionals must be found to help advise the organisations most in need.

Several organisations expressed a need and desire to reach out more effectively to the public and to better understand their audience, and from there to calculate how best to address their particular situation and take the next steps, but lacked the requisite information and tools to do so.

In this sense, as with other areas, peer-to-peer learning is integral. A goal of the envisaged Network is to increase ties between its constituent organisations and where possible organisations with greater capacity in the Network. With possible additional assistance from the client as well, significant advances can be made in this area.

Upskilling to Upscale:

Annex B

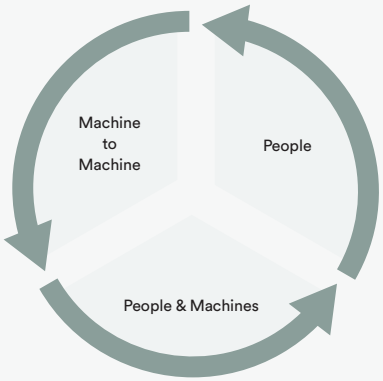
RISK MANAGEMENT FRAMEWORK

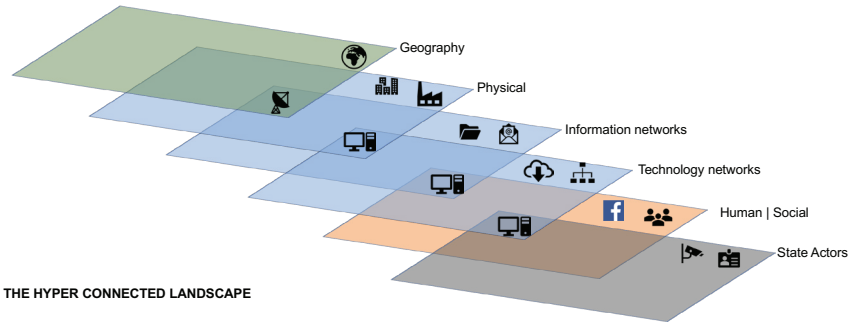
1. INTRODUCTION

Given the project mandate, the operating environment (with threat actors therein) and the future nature of work to be conducted, risk management has constituted a significant component of everyday business and it will continue to do so as the Network expands and progresses.

In order to both identify and understand potential risks associated with organisations being considered for inclusion in the Network, we undertook an All Threats All Hazards (ATAH) assessment, of which a Network partner due diligence exercise composed a significant part. This has helped us better understand whether potential partner organisations were suitable for inclusion, what threats they face and what potential risks need to be mitigated in order for the Network to function securely. The ATAH model was chosen due to the fact that the project and Network exist within a hyper-connected environment[1], where the threats, hazards and associated risks are multiple, often intrinsically linked and heavily technology focused. This results in multi-spectrum interactions between:

In the context of the Network operating environment this hyper-connectivity landscape could be visually interpreted as:





THE HYPER CONNECTED LANDSCAPE

[1] This landscape is based upon the US and UK MODs model, and BS 31111:2017 Cyber Risk and Definition, definitions as given by DA Resilience Ltd.

[2] Definition in part based upon advice provided by DA Resilience Ltd.

1.1 ATAH.

The concept of an ATAH model[2] is based on military and security intelligence good practice. It provides a useful framework in this hyper-connected environment to collect, analyse, disseminate and direct information in order to support design, decision making and action in the risk management spectrum of operations.

1.1.1. DEFINITIONS OF RISK, THREATS AND HAZARDS.

Threats and Hazards may lead to the same, intrinsically linked or similar consequences or impacts when considering holistic risk. Risk is defined as 'Likelihood x Impact'. Likelihood and resulting consequences will vary depending on whether the cause is from a Threat or Hazard. For the purposes of this project ATAH model the following will be used to describe Threats and Hazards:

- **Threat:** The actions of a malicious actor, who has the capability and intent to misuse, attack or disrupt the integrity or availability of information / data, operational technology, and humans. Malicious actors will seek to exploit or create vulnerabilities across the spectrum of operations, especially in the technological or human components. In the case of the Network, both these actions will have a physical safety (assets and humans) and security (assets, humans and technology) impact.
- **Hazard:** A physical, information or technological impact arising from a vulnerability in humans (non-malicious actors), processes and/or technology.

1.1.2. DEFINITION OF MALICIOUS ACTORS.

The following actors are viewed as likely malicious actors in regard to the Network, all of whom, depending upon intent, can become intrinsically linked:

- **State Actors:** State actors will have significant time (strategic patience) and capability to develop and insert threats, be it in the human or technological spectrum of operations. These threats can manifest themselves in the form of espionage (intelligence or information gathering) or offensive operations (degrading or disrupting organisational operations or personnel).
- **Criminal Networks:** Criminals conduct the overwhelming majority of cyber-attacks, be it for theft, ransom or fraud, and they are often extremely tech-savvy. The nexus that exists between nation states and the use of cyber criminals to advance state activity cannot be excluded from the analysis.
- **Network Partner Insiders:** Employees, whether malicious or non-malicious, can pose some of the greatest risk due to their potential access and the fact that all humans are in some way pliable and open to bribery or blackmail scenarios. In addition, one cannot ignore the potential actions of a disgruntled employee, or general ignorance. In the context of the Network, we have viewed this risk as being greater in larger organisations where there is arguably less managerial focus due to capacity, or where there is less peer-to-peer familiarity.

ANNEX B: RISK MANAGEMENT

1.1.3. ASSUMPTIONS.

In the context of this project and the Network, vulnerabilities can result from, but are not limited to, weaknesses in the following areas:

- Human component
- Organisational governance
- Operational practices
- Technology
- Physical infrastructure
- Organisational Security

OR

PEOPLE
PROCESSES
TECHNOLOGY

People, processes and technology all have inherent vulnerabilities, which can be exploited by malicious attack, or lead to a non-malicious incident. With regard to the Network, all three play a significant role.

- **People:** All people are susceptible, in varying degrees, to influence and manipulation by malicious actors and there exists the risk of process circumvention by staff. Open-source social media, state assets and the dark web can all be put to use to research individuals, who can be vulnerable to a Social Engineering attack.
- **Process:** There will always be gaps and vulnerabilities in process, regardless of organisational size or capacity, which will often be exploited by malicious actors in the first instance. These might include the lack of resourced capability to manage competent process implementation or management, sloppy IT security protocols, or a lack of threat awareness, education and training.
- **Technology:** All IT systems have inherent flaws, all of which are often intrinsically linked to people and process. In addition, given the pace of development in the technology sector there will rarely be a period where software and hardware are absolutely secure and beyond penetration.

1.1.4. DUE DILIGENCE.

As part of the assessment and analysis phases we chose to conduct in-house and independent expert due diligence against the potential partner organisations. The primary objective of the due diligence was to understand and mitigate any potential or existing vulnerabilities that the organisations being considered for inclusion in the Network might have to Russian influence. Following consultation with sources based in country, country-specific subject matter experts, and a review of open and public sources, the following areas were examined:

- Corporate verification: an assessment of the authenticity of the organisation
- Key individuals: an assessment of who is behind the organisation, and whether they appear legitimate or could bring a risk of disrepute to the organisation

ANNEX B: RISK MANAGEMENT

- Political exposure to Russia: whether there is existing Russian exposure, and if so, what the nature of that exposure is; if not, whether there are any possible or probable vulnerabilities to future exposure
- Litigation: an assessment of whether the entity has faced any issues with lawsuits (for example, defamation, resulting in public retractions or apologies)
- Donor conflict of interest: an assessment of whether there any existing or potential donor conflicts of interests (i.e. does the entity simultaneously accept money from Western and Russian or Russian-influenced donors)
- General integrity

1.1.5. METHODOLOGY.

The findings outlined here are based on a comprehensive review of the aforementioned sources, as well as from public source and proprietary databases.

Moreover, trusted sources within region-specific human source networks provided information regarding the integrity of these entities. These sources are well placed to hear and report any rumours regarding potential Russian influence. Sources accessed include Western investigative journalists and other media subject matter experts, academics, diplomatic sources, NGO and civil society assets, and knowledgeable sources in international organisations.

In addition, research was conducted on the potential influence that geography and the prevailing socio-political conditions have on Network partners, and whether this translates into increased levels of risk to the organisation or operating risk for the Network. This information was open source and focused predominantly on domestic political environments, Russian influence in these political systems (both contemporary and historical), and whether there is evidence to suggest that current and future political developments are likely to be subject to Russian interference.

Furthermore, the risk to Network partners of exposure or undue influence or coercion through bribery and corruption, or through the actions of nation state actors, was examined in the context of their geographical location. There is significant evidence for these practices in Russia's 'near abroad', in part due to the legacy of Soviet regional hegemony. With this in mind, we chose to not approach law enforcement or security services, or potentially compromised government officials, in the course of our human source enquiries, especially given the potential for partner exposure.

A summary of the due diligence findings can be found as an Appendix to this Annex.

B

ANNEX B: RISK MANAGEMENT

2. CURRENT SITUATION: RISK ENVIRONMENT

It has been somewhat challenging to understand 'ground truth' in the context of the security environment given the varied response from prospective Network members to the information gathering exercise. Despite this, the combination of what was received and the research conducted online and physically by team members has provided enough context to make a worthwhile assessment of the risk and ergo the security environment. The following major themes have been identified:

- There is significant operational diversity and varying competencies at the organisational level.

- The highest risk to Network performance lies within the electronic and technological spectrum. There remains risk to personnel, but much of this is predominantly geography-dependent from the standpoint of the reach and influence of Russian activity. As a result, the Risk Management framework will focus heavily upon solutions within the technological spectrum.

- Geography plays a significant part in determining the various threats, risks and responses. Simply put, the closer one is to Russia, or to a state that has a history of Russian interference, the greater the likelihood that threats are physical in nature.

3. KEY FINDINGS: RISK ENVIRONMENT

3.1. OPERATIONAL ENVIRONMENT.

The risk environment is extremely 'active' with organisations reporting a variety of risks associated with the work they do. Working with the ATAH principles, we view the following as a current situation analysis and assessment of the Risk Environment:

B

ANNEX B: RISK MANAGEMENT

THREATS & HAZARDS	VULNERABILITIES & EXPLOITS	ORGANISATIONAL IMPACT
A	B	C
MALICIOUS ACTORS: • State sponsored security services • Government • Cyber criminals • Insider threat from current and former employees and contractors NON-MALICIOUS FAILURES: • Human errors • Technology failures • Process failures • Culture	ORGANISATIONAL: • Employees • Technology platforms • User devices • Computers • Infrastructure • Applications • Communications portals • The Network • Lack of operational awareness EXTERNAL: • Third Party service providers, including all of the above • Information source networks • Family and friends • Home security PHYSICAL EXPLOITS: • Removal, denial or manipulation of information • Operational capacity degradation or denial • Vector pivot to another connected target • Bribery, compromise or intimidation	OPERATIONAL INTEGRITY: • Loss in capacity and capability • Degraded mandate • Asset degradation REPUTATION & OPERATIONAL INTEGRITY: • Loss in partner confidence • Loss in source confidence • Trust issues • Professional reputation HUMAN: • Recruitment and engagement • Privacy • Safety and security • Friends and family safety and security • Medical / loss of life • Intimidation / fear • Professional marginalisation • Loss of reputation • Psychological impact FINANCIAL & LEGAL: • Litigation costs • Funding withdrawal • Asset denial • Compensation claims • Insurances • Compliance costs • Security infrastructure costs • Technology recovery costs • Technology upgrade costs • Regulatory fines: data breach / loss of personally identifiable information
MALICIOUS ACTORS – STATE ACTOR AND CRIMINAL CHARACTERISTICS **Behaviours**: For the purposes of the project these are considered to be host nation security services or Russian actors, or a combination of both. Significant capacity, capability and reach, including: • Strategic patience • Demonstrated intent and capability • Will form alliances, even with criminal elements • Morally ambiguous • Operations can be overt or designed to ensure anonymity • Significant operational endurance and assets • Ability to exploit the entirety of the hyper connected landscape and spectrum of operations (PPT)		
PHYSICAL EXPLOITS: • Removal, denial or manipulation of information • Operational capacity degradation or denial • Vector pivot to another connected target • Bribery, compromise or intimidation	PHYSICAL EXPLOITS: • Removal, denial or manipulation of information • Operational capacity degradation or denial • Vector pivot to another connected target • Bribery, compromise or intimidation	PHYSICAL EXPLOITS: • Removal, denial or manipulation of information • Operational capacity degradation or denial • Vector pivot to another connected target • Bribery, compromise or intimidation

B

ANNEX B: RISK MANAGEMENT

3.2. IDENTIFIED RISKS.

The following risks have been identified during the period of research, all of which have happened in the near past or are current and daily:

- Online trolling and defamation
- Hacking and data breaching
- Physical and emotional harassment
- Physical attacks against personnel
- Litigation actions as part of ongoing efforts to disrupt counter-disinformation campaigns
- Bribery or 'kompromat' scenarios

3.3. RISK INFLUENCE / EFFECT.

The above-mentioned activities are influenced, enhanced or mitigated by the following factors, all of which are intrinsically linked:

- The size of the organisation. In broad terms, the smaller the organisation, the less well prepared they are to cope in the risk environment.
- Their geographical location. Geography influences the severity of the risk environment, especially when dealing with physical and personnel risk.
- The organisational understanding of the threat and risk environment. In broad terms, the smaller the organisation, the less likely they are to invest in formalising their approach to risk and organisational security.
- Funding. The smaller the organisation, the less likely they are to have a developed formal risk security management processes or plan to mitigate risk, or the assets to combat external interference. An increase in funding could mitigate this problem.

4. CONCEPT NOTES: NETWORK RISK MANAGEMENT

A central part of this report has dealt with security, principally cyber security. In this overview we will present general recommendations on some of the security and risk management considerations in light of the approach taken during the project and some of the factors that the project team experienced during the project. This section will not focus upon the technological requirements as these have been touched elsewhere, but it will seek to provide greater context on some of the operational management considerations.

B

ANNEX B: RISK MANAGEMENT

4.1. GENERAL.

The sheer size of the project geography, including the number of potential partner organisations, has dictated the construct and management of the risk management component during the project. As a result, there is a need for focus and efficiency in key areas set against the fact that there is simply not enough capacity or funding to provide technical or physical security uplifts to all the organisations. Therefore, the following was necessary and is suggested:

- Strong focus upon building a simple, flexible and cost effective secure information sharing network that has functionality
- Cyber threat management and reporting
- Training, mentoring and education to increase operational security awareness
- Provision of security threat reporting and analysis
- Physical security support
- Source network analysis and independent due diligence
- Consider the human impact of operating in the Network jurisdictions

4.2. NETWORK HEADQUARTERS.

A Network headquarters should be established, which should be viewed as an independent entity separate from the normal workings of the parent organisation and subject to stricter security controls than might otherwise be expected. As a base minimum, the following should be considered:

4.2.1. LOCATION.

Central Europe presents the most viable option for the headquarters. There is no single location that is most suitable given the geographical spread of Network partners, but any location for the headquarters should have access to excellent regional transport links in order to close this geographical gap. In addition, consideration should be given to host nation security and susceptibility to Russian influence. Due consideration can be given to a jurisdiction that lends greater corporate opacity to any structure moving forward and which provides, possibly through a subsidiary, greater 'corporate firewalling' against litigation and disruption efforts.

ANNEX B: RISK MANAGEMENT

4.2.2. BUILDING.

The headquarters should consider being located in a nondescript building that avoids attention. Its presence should not be advertised. There must be strict access controls in place utilising the following security measures:

- Reinforced airlocked doors with access pass systems in place
- CCTV
- Segregated server room and, where possible, direct control over the main switch for network access. If not possible, suitable firewalling measures to be in place to control external access to internal networks
- Server room can double up as a safe room, if needed
- If possible, an internal segregated meeting room or communications room for sensitive briefings and conference calling
- All windows to be tinted from external view
- Technology uplift in line with the advice provided in the Information Sharing Framework section of this document (Annex C)
- Access to internal staff kitchen and amenities
- Any external security or building management provided by contractors to be vetted prior to occupation

4.3. PERSONNEL.

Across the spectrum of operations, including Network partners, staff represent high risk and should be managed accordingly. This was a driving factor behind conducting the levels of due diligence on the organisations and ascertaining their suitability or potential exposure to undue influence. Given the nature of the threat and hazards the following is suggested:

- All employees and partners subject to national security vetting or independent third-party vetting with a focus on integrity and political exposure
- Develop open source vetting protocols on employee online presence and a framework for mitigating vulnerabilities and over exposure and potential exploit through social media
- Develop peer to peer networks aimed at identifying out-of-place or suspicious behaviours in staff.
- Establish close liaison protocols with network partners in order to identify new staff and associated changes in the partner structure. If necessary, conduct independent vetting on the organisations in order to maintain integrity.

4.4. OPERATIONS MANAGEMENT.

The operating environment remains complex and fluid. Given the nature of the country risks and widespread exposure to multiple threats and hazards there is a need for robust risk-focused operations management that is staffed and managed accordingly, but which does not stifle productivity. The following is suggested:

B

ANNEX B: RISK MANAGEMENT

4.4.1. QUALIFIED PERSONNEL.

We suggest the security effort is resourced with qualified personnel. Given the nature of the network and the strong focus upon security the following individuals are considered vital:

- **Security Officer:** former military or security services with a developed understanding of the operating geography and technological component. Training and mentoring skills also necessary. Ability to write and present coherent framework policies and documents
- **Deputy Security Officer:** former military or security services with a developed understanding of the operating geography and technological component. Training and mentoring skills also necessary. Ability to write and present coherent framework policies and documents
- **IT Security Officer:** training and mentoring background. Ability to write and present coherent framework policies and documents
- **IT Security Technician:** training and mentoring background

4.4.2. CODE OF CONDUCT

Establish a legally enforceable code of conduct and ethics in order to enhance compliance and integrity across the Network.

4.4.3. PROTOCOLS FRAMEWORK

Establish a coherent protocols framework aimed at delivering operational safety to all participants, and which is harmonised across the spectrum of operations. This should include, but is not limited to:

- Network communications and information transfer
- Use of devices and applications
- Storage of information and data
- Personnel security
- Crisis response mechanisms and management
- Network IT and Operations security protocols
- Lessons learnt
- Information and intelligence sharing on malicious actor activity
- Employee and partner vetting
- Insider threat reporting and whistleblowing protocol
- Public facing and social media online presence protocols, to include ‘pat lines’ and post-employment briefing notes (perhaps only pertinent to headquarters staff)

ANNEX B: RISK MANAGEMENT

4.4.4. REPORTING MECHANISMS

Establish reporting mechanisms that inform the wider Network as to the following:

- Cyber threat management and reporting: this could be enhanced if AI software is a component part of the programme
- Continued risk assessment and analysis: this would inform a periodical security briefing but can also be used to brief partners of imminent issues or areas of weakness

4.5. ADDRESSING OTHER THREATS AND HAZARDS.

Taking into account the legal, socio-political and multiple security risks previously described, the following is also suggested:

- External data storage facilities located in a country of low risk
- Provision of operational security training and mentoring focused on the following areas:

    - A 'Network induction' briefing programme that establishes basic benchmarks and expectations on the current operating situation and security environment. Refresher training quarterly or as operational situation dictates
    - Operational security: IT and personnel
    - Provision of security support services to less well-established Network partners. To include IT and personal security briefings but also physical or IT infrastructure surveys and recommendations
    - Independent verification of source networks or individuals: a due diligence service to ensure that we maintain information and partner integrity
    - Access to independent legal advice, especially in addressing physical acts of harassment, intimidation and injury
    - Develop an independent information monitoring service. Underpin this with a crisis management public engagement strategy aimed at disrupting malicious actor intent and triggering timely responses from governments
    - Provide access to specialist counselling and support, especially in addressing physical acts of harassment, intimidation and injury or psycho-social threats
    - Establish protocols and methods to securely transfer funds to partners operating in high risk areas. In so doing, ensure there is sufficient legal understanding of legislation in said areas and what the implications are for receiving funding from foreign sources

B

ANNEX B: RISK MANAGEMENT

APPENDIX 1 TO ANNEX B

The following tables are presented according to the reports prepared by our independent due diligence analyst, for ease of cross-reference.

As a result of due diligence, and discussions internally and with the client, three organisations – Propastop of Estonia, Faktograf of Croatia and Demagog of the Czech Republic – were removed from consideration for inclusion in the Network.

It was not considered necessary to conduct due diligence on DFRLab, a project of the Atlantic Council. The Kosciuszko Institute of Poland has been provisionally included in the list while a full due diligence report remains pending.

1. SUMMARY OF DUE DILIGENCE FINDINGS

1.1. GROUP A: BULGARIA, SERBIA AND ESTONIA:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
PROPASTOP	ESTONIA	LOW	LOW	LOW
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY (ICDS)	ESTONIA	LOW	LOW	MEDIUM
CENTER FOR THE STUDY OF DEMOCRACY (CSD)	BULGARIA	LOW-MEDIUM	HIGH	MEDIUM-HIGH
BULGARIA ANALYTICA	BULGARIA	LOW-MEDIUM	MEDIUM	MEDIUM
CENTER FOR EURO-ATLANTIC STUDIES	SERBIA	LOW	HIGH	MEDIUM
ISTINOMER	SERBIA	LOW	HIGH	HIGH
KRIK	SERBIA	LOW	HIGH	HIGH

1.2. EXECUTIVE SUMMARY OF GROUP A:

1.2.1. There are concerns over both Estonian organisations, especially Propastop, which has ties to both the Estonian government and neo-fascist groups. Sources indicate that Propastop has been involved in inciting violence against Estonia's Russian minority. Its reporting is widely considered to lack credibility and they have published a number of intentionally false and defamatory articles about Russian media outlets.

ANNEX B: RISK MANAGEMENT

1.2.2 The ICDS is funded by and politically linked to the Estonian state, specifically the Ministry of Defence, giving the appearance of independence without being so. It is more respectable than Propastop, and is not linked to the far right, though it reflects the hawkish nationalism of the Estonian government.

1.2.3 There is no evidence, and low risk, of Russian interference in any of these organisations. However there is a chance, particularly in Serbia, that litigation might be initiated against members by pro-Russian bodies or individuals.

1.2.4 While there is no open evidence of Russian support for the Bulgarian organisations, Russian interests do attempt to exert influence in the country via the distribution of funds 'under the table'. Neither Bulgaria Analytica nor CSD has been identified as a likely Russian conduit, but this does not eliminate concerns about associated individuals. Bulgaria Analytica's funding is notably opaque.

1.3. GROUP B: LATVIA, LITHUANIA, UKRAINE, POLAND, BOSNIA, CROATIA, ROMANIA:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
CENTRE FOR EAST EUROPEAN POLICY STUDIES	LATVIA	LOW	HIGH	HIGH
DELFI	LITHUANIA	LOW	HIGH	HIGH
LAISVES TV	LITHUANIA	LOW	HIGH	HIGH
DETEKTOR MEDIA	UKRAINE	LOW	HIGH	HIGH
WARSAW INSTITUTE	POLAND	LOW	MEDIUM	MEDIUM
FUNDACJA REPORTERÓW	POLAND	LOW	MEDIUM	LOW-MEDIUM
WHY NOT	BOSNIA	LOW	MEDIUM-HIGH	MEDIUM-HIGH
FAKTOGRAF	CROATIA	LOW	HIGH	HIGH
RISE PROJECT	ROMANIA	LOW	HIGH	HIGH
GLOBAL FOCUS	ROMANIA	LOW	MEDIUM	MEDIUM

ANNEX B: RISK MANAGEMENT

1.3.1. EXECUTIVE SUMMARY OF GROUP B:

- There are no significant concerns over any of the above organisations.
- The Warsaw Institute, while officially independent, is widely understood to be under the control of Poland's governing Law and Justice Party (Prawo i Sprawiedliwo**sc** PiS), and to sit to their right politically. It has an avowedly anti-Russian bias and there are no concerns of any risk of Russian influence.
- Fundacja Reporterów is linked to Poland's opposition Civic Platform party. They have lost funding since the PiS came to power and there are serious questions over their ability to sustain normal business operations. There is also evidence to suggest that they have chosen to align their mandate with their ability to raise funds, raising valid questions over their integrity.
- The situation of the Polish organisations underlines a risk relating to entities that rely on public money, namely that their viability may be compromised by a change in government.

1.4. GROUP C: BELARUS, SLOVAKIA, MOLDOVA, POLAND, GEORGIA:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
EURORADIO	BELARUS	LOW-MEDIUM	HIGH	HIGH
SLOVAK SECURITY POLICY INSTITUTE (SSPI)	SLOVAKIA	LOW-MEDIUM	MEDIUM-HIGH	MEDIUM-HIGH
MEMO 98	SLOVAKIA	MEDIUM	HIGH	HIGH
GLOBSEC POLICY INSTITUTE	SLOVAKIA	LOW	MEDIUM	MEDIUM-HIGH
GRASS FACTCHECK	GEORGIA	LOW	MEDIUM	MEDIUM-HIGH
ASSOCIATION OF INDEPENDENT PRESS	MOLDOVA	LOW-MEDIUM	HIGH	HIGH
INSTITUTE OF PUBLIC AFFAIRS	POLAND	LOW	MEDIUM	MEDIUM
DEFENCE 24	POLAND	LOW	MEDIUM	MEDIUM-HIGH
CENTRE FOR INTERNATIONAL RELATIONS	POLAND	LOW	MEDIUM	MEDIUM-HIGH
SUT.AM	ARMENIA	LOW	HIGH	MEDIUM-HIGH

ANNEX B: RISK MANAGEMENT

1.4.1. EXECUTIVE SUMMARY OF GROUP C:

- There are no major concerns over any of the above organisations in regard to undue Russian influence.
- Memo 98 is the only organisation that has potential vulnerability to Russian influence, but this is due to its involvement in election monitoring, which could make it a target of Russian cyber-warfare
- GLOBSEC, SSPI and FactCheck are all associated with political elites in their home countries, meaning they are considered either clearly pro-government or pro-opposition. GLOBSEC has reportedly been involved in shaping Slovakian government policy, which impacts its domestic reputation.

1.5. GROUP D: MOLDOVA, SLOVAKIA, CZECH REPUBLIC, POLAND, U.K:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
NEWSMAKER	MOLDOVA	LOW-MEDIUM	HIGH	HIGH
ZDG	MOLDOVA	LOW	HIGH	HIGH
INSTITUTE FOR PUBLIC AFFAIRS (IFPA)	SLOVAKIA	LOW	HIGH	HIGH
PRAGUE SECURITY STUDIES INSTITUTE	CZECH REPUBLIC	LOW	HIGH	HIGH
DEMAGOG	CZECH REPUBLIC	LOW	HIGH	HIGH
CENTRE FOR PROPAGANDA AND DISINFORMATION ANALYSIS (CPDA)	POLAND	LOW-MEDIUM	MEDIUM	LOW-MEDIUM
CENTER FOR EUROPEAN POLICY ANALYSIS (CEPA)	POLAND	LOW	HIGH	MEDIUM
BELLINGCAT	U.K.	MEDIUM	MEDIUM	MEDIUM
FACTMATA	U.K.	LOW	MEDIUM	HIGH
INSTITUTE FOR STRATEGIC DIALOGUE (ISD)	U.K.	LOW	MEDIUM	MEDIUM

ANNEX B: RISK MANAGEMENT

1.5.1. EXECUTIVE SUMMARY OF GROUP D:

- These organisations are generally regarded as well established, independent and free from Russian influence.
- ZDG, which operates in the 'dual-threat' environment of Moldova, has been involved in numerous lawsuits but has yet to lose one. Its fellow Moldovan organisation, Newsmaker, is potentially vulnerable to Kremlin influence, given its general director's connection to pro-Putin oligarch Alisher Usmanov, though despite this it has to date remained consistently critical of both the Moldovan and Russian governments.
- There are some financial transparency concerns relating to Newsmaker, ZDG, and IfPA, who do not disclose their funding. There are also concerns that CEPA is a vehicle for US interests and is being used to influence Polish politics in a pro-US direction.
- Other concerns were that the CPDA and ISD had analytical shortcomings, and that Bellingcat was somewhat discredited, both by spreading disinformation itself, and by being willing to produce reports for anyone willing to pay.

1.6. GROUP E: LITHUANIA, LATVIA, GEORGIA, UKRAINE, SLOVAKIA, CZECH REPUBLIC, HUNGARY:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
LITHUANIAN ELVES	LITHUANIA	MEDIUM	MEDIUM	MEDIUM
RE:BALTICA	LATVIA	LOW	HIGH	HIGH
NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE	LATVIA	LOW	MEDIUM	HIGH
MEDIA DEVELOPMENT FOUNDATION	GEORGIA	LOW	MEDIUM	HIGH
STOPFAKE	UKRAINE	LOW-MEDIUM	HIGH	MEDIUM-HIGH
IRI BEACON PROJECT	BELGIUM / SLOVAKIA	LOW	HIGH	HIGH
EUROPEAN VALUES	CZECH REPUBLIC	LOW	HIGH	HIGH
CODA STORY	GEORGIA	LOW	HIGH	HIGH
POLITICAL CAPITAL	HUNGARY	LOW	MEDIUM	MEDIUM-HIGH
ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT	INTERNATIONAL	LOW	HIGH	HIGH

ANNEX B: RISK MANAGEMENT

1.6.1. EXECUTIVE SUMMARY OF GROUP E:

- This is a highly credible and reputable grouping of entities, which exhibit high levels of independence and integrity and low exposure to Russian influence. There are, however, minor concerns over Lithuanian Elves, StopFake, Political Capital and the IRI Beacon Project, all of whom suffer from credibility, capacity or independence issues.
- The Lithuanian Elves (also known as the Baltic Elves) have been extremely successful at exposing Russian media manipulations, but have been accused of fomenting anti-Russian prejudice and spreading falsehoods themselves. Their credibility inevitably suffers from the fact that they are volunteers, not trained journalists.
- StopFake has been criticised for a monomaniacal fixation on Russian hybrid warfare, but its work has been widely praised. While it does not itself appear vulnerable to Russian influence, its parent organisation, the Media Reforms Center, runs another project in association with Rinat Akhmetov, a Ukrainian oligarch with alleged ties to pro-Russian separatists in Donbass.
- Political Capital is established as a firm opponent of the ruling Hungarian right-wing government, having been politically close to their centre-left predecessors. Their analyses are considered of good to moderate quality, but they suffer from sensationalist responses to Orbán and Putin, and they have a relatively poor network of sources in Hungary and the wider region.
- The Beacon Project is an initiative of the International Republican Institute (IRI). Though purportedly nonpartisan, the IRI has close links to the US Republican Party and has been accused of supporting coups against elected leaders who oppose US foreign policy. The Beacon Project is well regarded, and third-party due diligence rated it as 'high' for both independence and integrity, but the involvement of the IRI potentially compromises its credibility.

B

ANNEX B: RISK MANAGEMENT

1.7. GROUP F: BULGARIA, SERBIA, ESTONIA, LATVIA, GERMANY, NETHERLANDS, ITALY AND SPAIN:

ENTITY	COUNTRY	RISK TO RUSSIAN INFLUENCE	INDEPENDENCE	INTEGRITY
HSSF FOUNDATION	BULGARIA	LOW	HIGH	HIGH
EUROPEAN WESTERN BALKANS	SERBIA	LOW-MEDIUM	MED	MEDIUM
NATIONAL CENTRE FOR DEFENCE AND SECURITY AWARENESS	ESTONIA	LOW	LOW	MEDIUM
LATVIAN ELVES	LATVIA	LOW	UNKNOWN	LOW-MEDIUM
CORRECTIV	GERMANY	LOW	MEDIUM	HIGH
CICERO FOUNDATION	NETHERLANDS	LOW	HIGH	HIGH
FANPAGE.IT	ITALY	LOW	HIGH	MEDIUM
PAGELLA POLITICA	ITALY	LOW	HIGH	MEDIUM
CIDOB	SPAIN	LOW	MEDIUM	HIGH
MALDITO BULO	SPAIN	LOW	HIGH	MEDIUM-HIGH

1.7. GROUP F: BULGARIA, SERBIA, ESTONIA, LATVIA, GERMANY, NETHERLANDS, ITALY AND SPAIN:

1.7.1. EXECUTIVE SUMMARY OF GROUP F:

- This is a highly credible and reputable list of organisations, with only peripheral concerns, relating to EWB and Latvian Elves, both of whom have credibility and capacity issues and, potentially, CIDOB.
- EWB does not disclose its funding publicly, making it difficult to determine the nature of its relationships with other organisations, most notably Tanjug, Serbia's state news agency, which is pro-Vucic and pro-Kremlin. No sources in Serbia consider EWB a Russian conduit, but it remains vulnerable to Russian influence given the nature of the Serbian media environment.
- In the case of Latvian Elves, they have links to the former head of the European security division of NATO, which throws their independence into question. Numerous high-profile journalists have indicated that their fact-checking capacity is questionable and their content often amounts to producing their own 'fake news' to send back into Russia.
- CIDOB has had question marks raised over its independence, given the fact it receives funding from local government. However, this allegation is widely rejected by numerous Spanish political commentators and experts, who consider CIDOB reliable, professional, and among the best think-tanks in Spain.
- Correctiv and Cicero both benefit from excellent reputations and are widely seen as highly effective organisations, perhaps the most impressive of all potential Network partners.

Upskilling to Upscale:

Annex C

INFORMATION SHARING PROTOCOL

C

ANNEX C: INFORMATION SHARING FRAMEWORK

1 INTRODUCTION

We set out to design an information sharing system to be operated by the Network Facilitator and used by all organisations included in the Network. On-site assessments and an information security questionnaire were used by a specialist risk advisor to determine the threat level and organisational capacity and capabilities of organisations. Based on the scope of the requirements and the information obtained from Network partners, we designed and built a solution using Microsoft Azure and Office 365. We set up and tested an Office 365 tenant using the hypothetical scenario and tested users to ascertain the right parameters for the system .

SUMMARY OF FINDINGS

There are large capacity and competency variations and gaps across the spectrum of Network partners. The Network Facilitator should note that this diversity extends deeply into the IT architecture of the Network partners and as such should acknowledge that any solution must have application across multiple IT platforms. It must be secure by design, easily malleable, easily managed and have application and purpose throughout the spectrum of Network partners.

We recommend that secure information sharing be achieved through a segregated secure online portal containing email, messaging, calling, video conferencing and data storage capabilities. Thus, potential data compromise could be prevented by securing the portal at every stage of the information sharing workflow. Ideally, access to the portal would be from designated encrypted workstations, themselves secured by robust physical measures such as access control on a segregated and monitored working space. Users should be required to complete vigorous training to ensure safe usage of this space, the workstation and the portal.

User access to the portal should be secured by two-factor authentication configured using designated encrypted mobile phones. The most secure option is that phones and workstations would be issued by the Network Facilitator but we recognize the cost implications and associated practicalities of this option. The paragraphs below set out the options and associated restrictions of using the portal via ‘Bring Your Own Device’ (BYOD) compared to Network-issued devices.

The information and data workflow itself should utilise strict rights management to protect data and communications from unauthorised access, both internally and externally. For example, policies and procedures could restrict email communication to whitelisted recipients and could employ capabilities such as ‘Do Not Forward’ and ‘Company Confidential’, to prevent onward sharing of communications, whether intentional or unintentional.

Where required, additional measures could be wrapped around this portal to monitor for and report against any threat of data leak. Artificial Intelligence tools could be used to inspect traffic, build up a pattern of user behaviour and flag any unusual activity.

These broad themes are explained in detail below, with the technical controls available, as well as the practical implications of applying such controls.

ANNEX C: INFORMATION SHARING FRAMEWORK

2 PLATFORM DESIGN

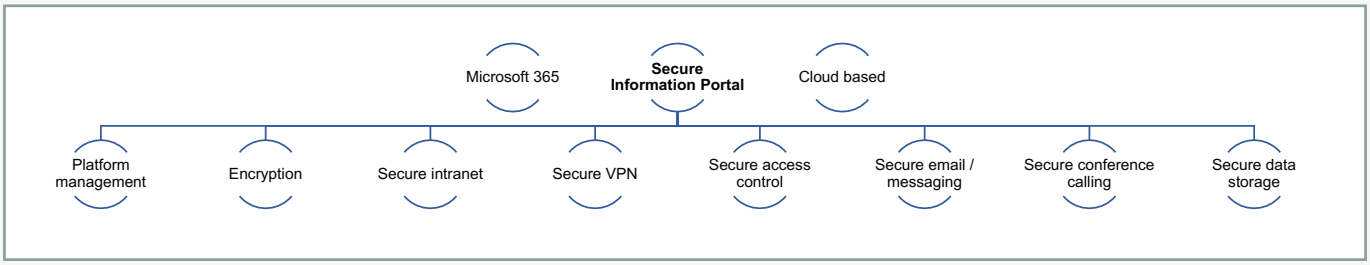
2.1. KEY TENETS

The platform solution has been shaped with the following key tenets at the heart of what is delivered:

- Relative simplicity
- Security
- Cost efficiency
- Ease of management
- Universal application

2.1.1 THE DESIGN

We recommend Information sharing be achieved through an online portal, containing email, messaging, calling, video conferencing and data storage capabilities. There are several solutions that could achieve this, however we recommend that the Network Facilitator uses an Office 365 tenant guarded with conditional access. This is because:



- • Most users are familiar with Microsoft Office and will be able to use the applications they recognise to document and communicate their activities.
- The Enterprise E5 subscription offers many of the advanced features that would be required by the Network for a relatively price-efficient fee, such as data loss prevention policies for email that help compliance enforcement.
- Microsoft Azure Rights Management is an additional add-on that is part of the Enterprise Mobility and Security License that applies on top of Enterprise E5. This tool allows restricted access to documents and email to only specific people and prevents anyone else from viewing or editing those files, even if they are sent outside the organisation.

The key to securing data is to strictly control every stage of the information workflow. As such, the use of Azure Rights Management is central to maintaining an audit of information and reducing the opportunity for that to be misused, mis-shared or stolen.

ANNEX C: INFORMATION SHARING FRAMEWORK

We recommend that features including message encryption and policies such as Encrypt Only and Do Not Forward which ensure that communications are encrypted, and onward forwarding of these messages is restricted and tracked are used. The use of advanced information protection means that data loss prevention and encryption is applied online for email, Skype for Business and SharePoint (where files can be stored). Thus, Network partners could keep all their content and communications within this secure information sharing portal, significantly lessening the risk of infiltration and data leak.

For the centralised management and control of Network user accounts, Azure AD could be automatically used as the backend of Office 365. Azure AD is a user directory that can centrally control access to all the resources inside the information sharing framework. The design would allow for Network partners to receive individual accounts that could be centrally managed by the network manager. Named accounts allow for accountability to individuals and auditing capabilities to track activity within the portal.

By using an integrated Microsoft system, a SharePoint site could be configured within this tenant. This could act as an Intranet where centralised information could be shared. For individual partner working, Microsoft applications could be utilised, but the functionality within these applications would be strictly controlled by Rights Management. For example, when opening a document, it is possible to add a banner to office applications that appears at the top of the document with its classification and instructions for use.

ISSUING DEVICES: AN EXTRA LAYER OF DESIGN

Access to this portal could be locked down further if using Domain Bound devices. This occurs in commercial enterprises where computers are connected to the central directory as authorised devices on that network. This means that users could restrict access to certain devices in certain locations. To achieve this, an external Active Directory, using AWS Active Directory Services, allows for two Windows AD Domain Controllers in the cloud. These would use Azure AD Sync to sync up to the cloud.

This design essentially creates a cloud based virtual private network (VPN) that manages access and services that are distributed remotely. Authorised devices could be issued to networked partners, who would use a VPN tunnel to a secure computer/network to bind to the Domain Controllers. The challenge with this aspect of the design is that it requires control over the end point devices.

The practical reality of this aspect of the design is that some of these organisations are already established and part of wider commercial entities. Issuing computers may not be possible or desired. Integrating with existing networks and systems would require access to internal IT, which may not be possible. As such, any platform must be configured to provide services that have cross system application, regardless of technology.

ANNEX C: INFORMATION SHARING FRAMEWORK

2.1.2 PLATFORM MANAGEMENT:

2.1.2.1 TECHNICAL SKILL REQUIREMENT

To develop this platform requires an IT engineer with significant skill in the Microsoft Cloud space. This level of experience is usually found in an engineer with at least ten years in the industry. The specific application of Information Rights Management is a complex area and requires specific understanding.

Rights Management is time consuming and requires an understanding of the full breadth of Microsoft Cloud functionality. Not only is technical skill required to configure, but so is an in-depth understanding of partner workflow in order to write appropriate templates for policies and apply them correctly. The potential of this tool is significant but would need investment in time and resource to set up.

2.1.2.2 HUMAN INVESTMENT

Training is undoubtedly required to successfully deploy and make use of this portal. This resource will need sufficient technical understanding to clearly explain the level of technical controls surrounding the portal, but also the personability to translate this to layman's terms and tutor Network partners as required.

Ongoing IT support is recommended, from basic requests surrounding user access, like password resets, to more complicated permissions setups. The management of permissions will also need to be coordinated by the network manager who should be aware of the range of work occurring across the Network and be able to make decisions on who should have access to what. Some files will be shared between Network partners, others will be specific to their respective organisations.

2.1.2.3 IT INFRASTRUCTURE INVESTMENT

Theinfrastructure is largely in the cloud, so economies of scale can be utilised. If the network manager chooses to go down the route of issuing managed devices, the infrastructure overheads increase considerably. This is because each device will need centralised management, from applying software updates to managing policies on the specific device, such as the ability to download additional applications.

2.1.2.4 TECHNICAL MANAGEMENT

Across all three management levels above, there needs to be a technical coordinator who has briefed the Microsoft specialists, who has an in-depth understanding of the Network partners and their specific requirements, and who has oversight of ongoing IT support. This management person or team would ultimately be responsible for the portal and its back-end infrastructure, as well as service delivery and the end user experience.

ANNEX C: INFORMATION SHARING FRAMEWORK

3 SECURITY CONTROL FEATURES

This section is about how the individual Network partner connects to the portal. It is concerned with user login, user location, and the type of device used to connect.

3.1 ACCESS CONTROL

Remote Conditional Access. Conditional access could be set up to only allow access from certain public IPs. This means that only the people behind those public IPs can access the Office 365 tenant. Where partners already operate from business premises, their commercial internet connections will provide a fixed public IP. IP addresses can be whitelisted, so that access to the portal can only occur from that location.

Where partners operate using a home grade internet connection, they may not be allocated a fixed public IP. It is easy to establish what public IP address a computer is using; users can simply Google 'what is my IP' or visit any number of websites that give that information. However, home grade internet service providers may have a pool of public IPs that they use for their customers, so it is possible that the public IP might change. Thus, whether this type of conditional access could be used across the board would require some investigation of the type of internet connections being used by Network partners.

The benefit of this type of conditional access is that the Network Facilitator could very clearly map where connections were being made from. Adopting a whitelist approach means that the network manager would not need to monitor traffic and identify anomalies, because any attempted connections that are not whitelisted would be automatically blocked. While it is possible to use VPN connections to obtain different IP addresses, it is almost impossible to spoof a specific public IP address because the connection requires a series of communications back and forth. Without fully controlling that public IP address, one could not receive traffic sent back to it, which would be required to secure the connection and bypass the access restrictions.

Device Access Control. When a user requests access to the information sharing portal, that user and their device is authenticated. If authentication is granted just on user account and password, the risk of account compromise is much higher. By deploying conditional access policies, access is granted only if the user conforms to the policy set out for the portal. New devices need to enrol in order to become trusted.

We recommend that multi-factor authentication be enforced for users to gain access to the portal. This works by associating a mobile phone and receiving a text message with a code for secondary authorisation to the account. Alternatively, Microsoft offers an authenticator app which is arguably more secure, because there is a small risk that text messages could be intercepted. An authenticator app requires a smartphone. Where organisations do not issue 'work' mobile phones, this would mean that individuals would be required to install the app on their personal phone.

Enforcing two-factor authentication would increase the security of the portal, as it would mean that a party could not gain access with the password alone. This mitigates the risk of an individual sharing, losing or saving their password somewhere it is compromised.

ANNEX C: INFORMATION SHARING FRAMEWORK

There are still risks posed by the potential for mobile phones to be lost or compromised themselves. It is hard to mitigate all these risks without also providing centrally managed phones that are also heavily locked down. Without providing mobile phones, certain BYOD policies are recommended, including requiring a password or 8-digit pin code on the device. Mobile security policies and training should also be rolled out to inform users of the importance of securing their devices and preventing unauthorised access.

Email Access Control. Further security settings can be applied to email via Exchange Online which supports different types of encryption:

- OME (Office 365 Message Encryption) could be used to encrypt all messages, both internal and external. OME works with other email services, including Gmail, but helps ensure that only intended recipients can view the message content. This tool allows the use of the application Do Not Forward for emails, or the prevention of the use of Reply All, for example.
- IRM (Information Rights Management) and AIP (Azure Information Protection) could be used to restrict the ability to download, copy, and print all documents and emails sent.

Document Access Control. Information Rights Management helps to classify, label and protect documents and emails. An administrator can configure rules to detect sensitive data, for instance. When a user saves a document that contains sensitive data, like credit card information, the application displays a warning message recommending a classification of 'Confidential' on that document.

Once the document is classified it is possible to track and control how it is used. It is possible to analyse the flow of data, detect risky behaviour, employ corrective measures, track access to files and prevent data leakage or misuse. When you have applied a classification to documents or emails, that classification is identifiable at all times, regardless of where the data is stored or with whom it is shared. The classification is embedded in visual markings, such as header, footer or watermark, but also in metadata added to files or emails.

ISSUING DEVICES: AN EXTRA LAYER OF ADDITIONAL ACCESS CONTROL

Domain / Device Access Control. Another method of conditional access is the requirement of the device to be joined to a domain. The benefit of domain-bound devices is the ability to centrally control these devices by applying policies, i.e. Windows group policy. It is also a method by which you can restrict access if the device is not bound to the domain, effectively whitelisting the authorised computers.

The difficulty of this is that computers need to be centrally controlled by the party running the Domain Controllers. As mentioned previously, if the Network partners already operate in a commercial environment, the likelihood is that their machines are already bound to their company domain. It is unlikely that they would want additional separate devices from which to access the information sharing portal.

The biggest challenge to conditional access is the assignment of hardware to users. If the contractor deploys hardware to all Network partners, it is possible to centrally manage devices and ensure compliance. If operating on a BYOD basis with enforced restrictions, then the scope and effectiveness of conditional access is lessened.

Application Access Control. If devices are issued by the Network, another layer of security can be applied in the form of application control which would be addressed by whitelisting only those applications required for the carrying out of Network activity.

All other applications could be disabled except for those deemed necessary to conduct the work required, such as Word, Excel, PowerPoint and SharePoint. While allowing desktop applications provides additional functionality, and therefore potential additional risk (such as the ability to copy and paste content), information rights management can still be applied on top of the applications to control data workflow, as described above.

Exchange Active-Sync should be blocked to prevent local sync of email accounts on any device. This would reduce the risk of data leak and mean that email could not be downloaded to mobile phones, although access to email is still possible through a browser, if that device is compliant and two-step verification is complete. While the mobile nature of business is recognised, security concerns prohibit organisations from operating with the degree of freedom to which they may be accustomed. It is anticipated that certain of these measures might be met with reluctance, and if this system if used, it will be imperative to explain the reasoning behind these policies to partners, in the context of the risks faced.

4 SECURITY AND COMPLIANCE

We recommend that alerts be configured to look for anomalous or suspicious behaviour based on login activity, file access and attempts to exfiltrate data.

Reports and dashboards could be set up as per IT Security needs for monitoring and compiling results. The extent of proactive monitoring would depend on the resource allocated to IT Security professionals carrying out this project.

Advanced Threat Protection could be deployed to protect the portal from multiple types of advanced cyber-attacks and insider threats. This tool detects multiple suspicious activities, focusing on several phases of the cyber-attack kill chain and presents these on a dashboard as Who, What, When and How. The dashboard could then be tailored to take specific types of action dependent on the results of certain reports, or the active monitoring and decision-making of IT security professionals managing the space.

Issuing Devices: an additional level of compliance. Microsoft Intune can apply various policies. A common use case is to restrict access to the cloud portal to managed devices. A managed device is a device that meets set standards for security and compliance, namely being under some sort of organisational control. Registering a device creates an identity for it in the form of a device object. This object can be tracked by the portal.

It is possible to authorise a device based on a unique identifier associated with the computer itself, called a media access control (MAC) address. So, as well as the public IP address denoting the specific location of the connection, the connection itself can be restricted to a specific computer. This can be achieved by using the MAC address of the computer, as this is the unique identifier associated with the network card of that machine.

The challenge of this approach is obtaining the correct MAC address from each individual computer that might require a connection. Dependent on the device, a computer might register multiple MAC addresses, i.e. one for its ethernet adapter and one for its wireless adapter. Where a computer requires a separate adapter to connect to ethernet, as MAC address. The risk here is that you can authorise the ethernet adapter, but then that adapter can be used on a different computer.

This is why several levels of authentication and authorisation are recommended because while there are opportunities to work around some methods, it is unlikely that a threat actor could compromise every layer of security.

5 CONCLUSION

From the research and testing conducted, it is clear that the Microsoft Cloud space contains many applications, tools and protections to achieve a secure information sharing portal that could be utilised by the partner Network. However, it is also clear that the variety of partners involved will mean significant preparation is required to develop and configure this platform in a way that will satisfy security requirements while complementing workflow and the varying levels of accessibility and locality.

The ultimate solution is a delicate balance between available finance and capability. As a base minimum, we recommend that the system is implemented including AI monitoring/reporting, less the physical issuing of workstation devices and mobile devices. Clearly, the issuing of centrally managed, encrypted devices is a gold-plated solution which can only be confirmed subject to a better understanding of the future financing lines. The base level Office 365 tenant should be layered with Azure Rights Management as the central tool in securing, auditing and controlling the flow of data. The potential of this solution is promising and the extent of functionality available in Microsoft, if deployed correctly, is sufficient to address the complex needs of this project.

Upskilling to Upscale:

Annex D

PROPOSED NETWORK MEMBERS

D

ANNEX D: PROPOSED NETWORK MEMBERS

	ORGANISATION	COUNTRY	ORGANISATION TYPE	OVERVIEW OF ACTIVITIES	PRIMARY AUDIENCES	LANGUAGE OF OUTPUTS	URL
BALKANS							
1	Why not	Bosnia	Grassroots implementor	Civil society organisation focused on creating a safe, efficient and responsible society. It was established as a youth peace organisation. It now aims to increase civic activism and government accountability. It also seeks regional demilitarisation.	General public, journalists, activists	Bosnian, english	Zastone.Ba/en/ca-why-not/
2	Bulgaria Analytica	Bulgaria	Media Outlet	The area that is of key interest to this network sits within Bulgaria Analytica but is called Center for Balkan and Black Sea Studies. This aims to understand the geo-economics of Russian and Western confrontation.	Policy makers, journalists	Bulgarian, English	bulgariaanalytica.org/en/
3	Center for the Study of Democracy	Bulgaria	Think Tank	Public policy institute dedicated to the promulgation of democracy. It has a strong Russia focus. It aims to provide capacity for a successful European integration process and monitor public attitudes with regards to institutional reform. Also works on anti-corruption and national security issues.	Civil society, journalists	Bulgarian, English	www.csd.bg/
4	HSSF Foundation	Bulgaria	NGO	Human and Social Studies Foundation. Its mission is to promote scholarly exchange in social and human sciences by implementing research projects, a publication program, and public debates.	Students, Government, Policy makers.	English	hssfoundation.org/en/aboaut-hssf/
5	Center for Euro-Atlantic Studies	Serbia	Think Tank	Civil society organisation that focuses on the development of the state and combating destabilising Russian influence on the Western Balkans.	Government, Policy makers, Journalists	English, Serbian	www.ceas-serbia.org/en/
6	European Western Balkans	Serbia	Web resource/ NGO	News portal on European integration and other EU-related topics in the Western Balkans.	Government, Policy makers, Journalists, General Public	English, Serbian	europeanwesternbalkans.com/
7	Istinomer	Serbia	Fact-checking Organisation	Serbian fact-checking organisation.	General public, journalists, activists	Serbian	www.istinomer.rs/
8	Krik	Serbia	Investigative Journalism Project	NGO operating as part of the Organized Crime and Corruption Reporting Project (OCCRP). Team of investigative journalists engaged in exposing crime and corruption.	General Public, Journalists, Government	English, Serbian	www.krik.rs/en/
CENTRAL EUROPE							
9	European Values Think Tank	Czech Republic	Think Tank	NGO devoted to fostering closer cooperation with the West. It does operational monitoring and analysis of disinformation and creates weekly reports on Czech disinformation. Also involved in policy development and advocacy, educational activities for the general public, training for practitioners, and public and behind-the-scenes advocacy for disinformation efforts.	Civil society, journalists, general public	English	www.europeanvalues.net/
10	Prague Security Studies Institute	Czech Republic	Think Tank	NGO devoted to promoting democratic, free market values in the Czech Republic and other post-communist states. It aims to build a community of security-minded policy practitioners. It identifies and analyses geopolitical flashpoints and emerging threats regionally and globally.	General public, journalists, activists	Czech, English	www.pssi.cz/
11	Political Capital	Hungary	Think Tank	Policy research and analysis consulting institute. It is committed to parliamentary democracy, human rights, and market economics. It focuses on issues including political risks, radicalism and extremism, electoral systems, and in particular, international relations between Europe and Russia.	Government, Policy makers, Journalists	English, Hungarian	www.politicalcapital.hu/
12	Center for European Policy Analysis	Poland	Think Tank	Non-profit dedicated to promoting strategically secure and politically free Central and Eastern Europe.	Policy makers, Government, journalists	English,	cepa.org/home
13	Centre for International Relations	Poland	Think Tank	NGO dedicated to deepening Polish decision-makers' knowledge of the EU and the world. No specific disinformation program.	Policy makers, government	English, Polish	csm.org.pl/en/home
14	Centre for Propaganda and Disinformation Analysis	Poland	Think Tank	NGO dedicated to combating information and psychological warfare.	Policy makers, Government, journalists	English, Polish, Ukrainian	capd.pl/en/

D

ANNEX D: PROPOSED NETWORK MEMBERS

	ORGANISATION	COUNTRY	ORGANISATION TYPE	OVERVIEW OF ACTIVITIES	PRIMARY AUDIENCES	LANGUAGE OF OUTPUTS	URL
CENTRAL EUROPE							
15	Kosciuszko Institute	Poland	Think Tank	NGO promoting the development and security of Poland within the EU and NATO. Runs the CYBERSEC Forum, devoted to the strategic issues of cyberspace and cybersecurity in Europe.	Government, Policy makers, civil society	English, Polish	cybersecforum.eu/en/
16	Defence 24	Poland	Media Outlet	Geared overwhelmingly toward military affairs	Policy makers, government	English, Polish	www.defence24.pl/
17	Fundacja Reporterów	Poland	Investigative Journalism Project	Investigative journalism/journalist training organisation with a focus on Ukrainian journalists.	General public, journalists, activists	English, Polish	fundacjareporterow.org/
18	Institute of Public Affairs	Poland	Think Tank	Think tank dedicated to policy research and analysis. Not actively combating disinformation.	Policy makers, government	English, Polish	www.isp.org.pl/
19	Warsaw Institute	Poland	Think Tank	Organisation dedicated to strengthening the position of the Polish state by providing analyses of economic policy, international relations, security policy, and the use of soft power.	Government, Policy makers, civil society	English, Polish	www.iimcb.gov.pl/en/
20	GLOBSEC Policy Institute	Slovakia	Think Tank	Think tank covering regional geopolitics, committed to increasing security. It aims to provide a better understanding of global trends and their consequences for society, security, and the economy.	General Public, Journalists, Government, Policy makers	English	www.globsec.org/
21	Institute for Public Affairs	Slovakia	Think Tank	NGO devoted to promoting the open society and democracy, analysing social, political, economic, legal, cultural, and foreign policy issues of public interest.	Civil society, journalists, general public	English, Slovak	www.ivo.sk/106/en/home
22	IRI Beacon Project	Belgium and Slovakia	Think Tank/Media Monitoring	Project focused strongly on Russian influence and disinformation.	Government, Policy makers, civil society	English	www.iri.org/web-story/beacon-project-shines-light-moscows-meddling
23	Memo 98	Slovakia	Media Monitoring and Assistance	Media monitoring organisation covering Eastern Europe. Was launched to monitor the Slovak media. Now focuses on media and elections.	General public, journalists, activists	English	memo98.sk/
24	Slovak Security Policy Institute	Slovakia	Grassroots Implementor	NGO devoted to security challenges and raising awareness of them. It connects security and defence policy experts from governmental, non-governmental, private and academic institutions. It focuses on research and analysis of security challenges, particularly with regards to cyber security.	Government, Policy makers, civil society	Slovak	slovaksecurity.org/
BALTICS							
25	International Centre for Defence and Security	Estonia	Think Tank	Think tank specialising in foreign policy, security and defence issues. Its mission is to strengthen Estonia's security and defence sector by identifying and analysing challenges and proposing policy solutions. Wants to sharpen strategic thinking in NATO and EU on security issues that affect the Nordic-Baltic region.	Policy makers, Government, journalists	English, Estonian, Russian	www.icds.ee/
26	National Center for Defence and Security Awareness	Estonia	NGO	NGO in Estonia dedicated to informing Russian speakers about national security and disinformation.			
27	Centre for East European Policy Studies	Latvia	Think Tank	NGO devoted to advancing Latvian foreign policy by building up expertise on Russia's regional behaviour.	Government, Policy makers, civil society	English, Latvian	appc.lv/eng/
28	Latvian Elves	Latvia	Network of Volunteers	Activist group targeting Russian disinformation.	General public, journalists, activists	N/A	N/A
29	NATO Strategic Communications Centre of Excellence	Latvia	Inter-governmental	Strategic communications for NATO.	Government, Policy makers	English	www.stratcomcoe.org
30	Re:Baltica	Latvia	Investigative Journalism Project	Centre for investigative journalism dealing with social and political issues.	General public, journalists, activists	English, Latvian, Russian	en.rebaltica.lv/
31	Lithuanian Elves	Lithuania	Network of Volunteers	Activist group targeting Russian disinformation.	General public, journalists, activists	N/A	N/A

D ANNEX D: PROPOSED NETWORK MEMBERS

	ORGANISATION	COUNTRY	ORGANISATION TYPE	OVERVIEW OF ACTIVITIES	PRIMARY AUDIENCES	LANGUAGE OF OUTPUTS	URL
BALTICS							
32	Delfi	Lithuania	Media Outlet	Major news portal for Lithuania, Latvia and Estonia.	General public, journalists, activists	English, Lithuanian, Russian	en.delfi.lt/
33	Laisves TV	Lithuania	Media Outlet	Lithuanian crowd-funded internet TV channel that streams in Lithuanian and Russian. 58,000 subscribers in Lithuania, 12.8 million views on YouTube.	General Public	Lithuanian, Russian	www.laisves.tv/
CAUCASUS							
34	Sut.am	Armenia	Fact-checking Organisation	Set up by the Union of Informed Citizens, a local NGO, dedicated to preventing the spread of obvious disinformation. Describes themselves as "number one fact-checkers in Armenia."	General Public, Journalists, CSOs.	Armenian, English, Russian	sut.am/
35	Coda Story	Georgia	Investigative Journalism Project	Network of journalists strongly focused on combating disinformation.	General Public, Journalists, Government, Policy makers	English	codastory.com/
36	GRASS FactCheck	Georgia	Fact-checking Organisation	Fact-checking organisation focused on Georgia and Russia-Georgia relations.	General public, journalists, activists	English, Georgian	grass.org.ge/en/
37	Media Development Foundation	Georgia	Grassroots Implementor	Journalist-founded, heavy emphasis on media literacy and human rights promotion, especially among young people.	Policy makers, Government, journalists, general public	English, Georgian	mdfgeorgia.ge/eng/home/
WESTERN EUROPE							
38	Correktiv	Germany	Investigative Journalism Project	Aims to make informative and investigative journalism available to citizens. Focuses on abuses of power and corruption in politics, and right-wing and religious extremism.	General Public, Journalists	English, German	correctiv.org/en/
39	Cicero Foundation	Netherlands	Think Tank/NGO	A forum for discussion of problems related to European integration.	Government, Policy Makers, Academics.	Dutch, English	www.cicerofoundation.org/
40	Bellingcat	UK	Investigative Journalism Project	Open-source investigative journalism project that reports on conflicts and criminal networks.	General Public, Journalists, Government, Policy makers	English	www.bellingcat.com/
41	Factmata	UK	Commercial enterprise	Tech start-up using AI and algorithms to fact-check material and highlight extremist content and disinformation.	Journalists, Government, Policy makers, commercial enterprises	English	factmata.com/
42	ISD	UK	Think Tank	Global counter-extremism organisation engaged in research, analysis, data management and capacity building.	Journalists, Government, Policy makers	English	www.isdglobal.org/
SOUTHERN EUROPE							
43	Fanpage.it	Italy	Media Outlet	News outlet with a focus on Italian and international politics.	General Public, Journalists.	Italian	www.fanpage.it/
44	Pagella Politica	Italy	Fact-checking Organisation	Monitors the statements made by Italian politicians in order to assess their veracity.	General Public, Journalists, Activists.	Italian	pagellapolitica.it
45	CIDOB	Spain	Think Tank	Think tank with primary research focus on intercultural dynamics, security, migration, development, and global cities.	Government, Policy Makers, Academics, Journalists, General Public.	English, Spanish	www.cidob.org
46	Maldito Bulo	Spain	Journalism/Media Monitoring	Monitors political discourse and information circulating on social media networks and uses data journalism techniques to verify it.	General Public, Journalists, Political community.	Spanish	maldita.es/malditobulo/

D

ANNEX D: PROPOSED NETWORK MEMBERS

	ORGANISATION	COUNTRY	ORGANISATION TYPE	OVERVIEW OF ACTIVITIES	PRIMARY AUDIENCES	LANGUAGE OF OUTPUTS	URL
EASTERN EUROPE							
47	Euroradio	Belarus	Media Outlet	Warsaw-based radio station devoted to disseminating independent news. Broadcasts to Belarus but has to operate in Poland due to Belarus being a 'dual-threat' environment.	General public, journalists, activists	Belarusian, English, Russian	euroradio.fm/en
48	Association of Independent Press	Moldova	Media Assistance	National resource centre devoted to promoting a free press in Moldova.	General public, journalists, activists	English, Romanian	www.api.md/
49	Newsmaker	Moldova	Media Outlet	Primarily Russian-language online news source.	General public, journalists, activists	Romanian, Russian	newsmaker.md/
50	ZDG	Moldova	Media Outlet	Primarily Romanian-language online news source, specialising in investigative journalism.	General public, journalists, activists	Romanian, Russian	www.zdg.md/
51	Global Focus	Romania	Think Tank	Organisation dedicated to reform and state-building, cognizant of the threat of propaganda and disinformation.	Policy makers, Government, journalists, general public	English	www.global-focus.eu/
52	RISE Project	Romania	Network	Network of journalists, programmers and activists, investigating organised crime and corruption in Romania and abroad, and revealing hidden connections between criminal organisations, politicians and business.	General public, journalists, activists	English, Romanian	www.riseproject.ro/
53	Detektor Media	Ukraine	Media Outlet	Ukrainian news source	General public, journalists, activists	Ukrainian	detector.media/
54	Stop Fake	Ukraine	Investigative Journalism Project	Project set up by journalists, academics activists, dedicated to debunking 'fake news'.	General public, journalists, activists	Various	www.stopfake.org/en/news/
INTERNATIONAL							
55	DFRLab	Think Tank / Media Monitoring		Set up by the Atlantic Council, conducting open-source research to help people understand disinformation and build digital resilience. Tracks global disinformation campaigns and investigates war crimes and ceasefire violations in Syria and Ukraine.	General Public, Journalists, Policy Makers, Government.	English	www.digitalsherlocks.org/dfrlab
56	Organised Crime and Corruption Reporting Project	Investigative Journalism Project		Investigative reporting platform and consortium formed by 40 non-profit investigative centres, scores of journalists and several major regional news organisations. Mission is to educate on how organised crime and corruption resides in various countries and in their governments.	General Public, Journalists, Government, Policy makers	Various	www.occrp.org/en

Upskilling to Upscale:

Annex E

REGIONAL REPORTS

E

ANNEX E: REGIONAL REPORTS

1 BALKANS

1.1 SUMMARY OF FINDINGS

The Balkans region is complex. It combines EU and non-EU states, has a history of comparatively recent war in its western part that lives on in the regional consciousness, and a complicated, ambivalent relationship with Russia. These three factors inform both the geopolitical landscape and, accordingly, the nature of the disinformation and counter-disinformation battle being fought out here.

The organisations interviewed in this region come from three countries: Bosnia (Raskrinkavanje, which runs 'Why Not'), Bulgaria (Bulgaria Analytica, The Center for Study of Democracy, HSSF) and Serbia (Center for Euro-Atlantic Studies, European Western Balkans, with Istonomer to come). Each faces a clear overarching threat from Russian disinformation designed, broadly, to (1) draw it away from Europe and specifically the EU, and (2) entice it into Russia's orbit. Propaganda is both narrative-based and financially-linked and, where possible, geared to using local governments and state media as conduits or allies.

A critical point, and one that it is vital that the network as a whole internalises, is that the pro-Russia narratives here are often either subsumed within or subservient to broader anti-Western and anti-democratic narratives. These tend to focus on EU 'decadence', especially with regards to LGBT rights and lax borders, the atrophying of EU institutions, and the need for strong national leaders as opposed to faceless bureaucrats in Brussels

The seven organisations interviewed were all extremely aware of, and alert to, the Russian disinformation threat and showed a thorough understanding of its nuances, both at the semantic level (the language of specific narratives) as well as the dangers of corruption and the weaponisation of finance.

Without exception, all organisations interviewed expressed a need for greater capacity building, increased human and financial resources and assistance with big data science and social media analysis.

1.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

Bosnia, Bulgaria and Serbia are all 'dual-threat' environments, which is to say they face the twin threats of Russian propaganda and a hostile government and mainstream (often state) media. Russian propaganda is therefore a part of the media ecology across the Balkans.

In Bulgaria, pro-Russian attitudes are inscribed into national myths because of Russian successes against the Ottomans. In addition, the fall of the Iron Curtain was not greeted with the same enthusiasm as elsewhere in Eastern Europe, and a pervasive nostalgia for life under communism continues to endure. This atmosphere allows Russian disinformation to flourish.

In Serbia, Russia has infiltrated the media ecosystem through the arrival of the Sputnik news agency in 2014. Few people read Sputnik but many Serbian outlets use it as a source, often due to lack of resources. The Serbian media is happy to depict Russia as the 'good guy' to a population receptive to narratives of historical friendship. Many Serbs see Russia, a fellow Orthodox country that uses a shared Cyrillic script, as a friendly and powerful ally. As such,

ANNEX E: REGIONAL REPORTS

Serbian nationalism and Russophilia are almost one and the same. Today, Russia is seen to be supporting Serbia in the dispute over Kosovo, which is true.

A powerful narrative that plays on Serbia's traumatic history centres on portraying Putin as a strongman who would never have allowed Serbia to be bombed by NATO forces in 1999, in contrast to the pliant drunk Boris Yeltsin.

In Bosnia, Russia has used a similar tactic, by finding a local partner in the form of the government of Republika Srpska. The biggest 'Russian propaganda' outlet in Bosnia is in fact state media, in the form of Radio Televizija Republike Srpske.

The threat here is particularly acute as local governments, media and oligarchs act as incubators, enablers and, often, outright facilitators of Russian disinformation. This is a vital space for the network.

1.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

1.3.1 DEVELOPING RESEARCH PRODUCTS

Bulgaria Analytica is very strong in this area: it claims to be "second to none" in Bulgaria, and is particularly strong in followng what Russia does in Europe. Recent projects include looking at Russia's use of energy to permeate European political systems. Bulgaria Analytica believes that Serbia and Macedonia are very important arenas in this battlefield.

The Center for Study of Democracy (CSD) also maintains a strong presence here. Its in-depth report 'The Kremlin Playbook' is a good example of its activity. The CSD is not only developing products but new methodologies, such as creating a state capture risk index, based on both hard and soft data. that allows them to assess the level of state capture across the country.

HSSF is engaged in media monitoring. It identifies pro-Russian talking points and measures the frequency with which they occur in the Bulgarian online media. They recently published an in-depth report examining the period 2013-2016 and are now working on a follow-up report looking at 2017. The reports are published on news websites and blogs and on their own website.

The Center for Euro-Atlantic Studies specialises in professional analysis and reports with clear sources and references countering Russian disinformation "that no one can challenge and debunk."

European Western Balkans has also engaged in several large research projects in this area.

Raskrinkavanje claim some capacity in this area and have a long-term project devoted to daily monitoring of media in Bosnia and the wider region.

ANNEX E: REGIONAL REPORTS

1.3.2 FACT-CHECKING

Bulgaria Analytica claims that in some instances, they are doing the work that the security services should be doing. They operate the Center For Balkan and Black Sea Studies (CBBSS), a news aggregator that produces summaries of news reports and analysis as well as some field reporting. Much of the content is translated into Bulgarian.

HSSF is not especially geared toward fact-checking, focusing on 'overarching narratives rather than 'fake news'.

European Western Balkans has undertaken a project in conjunction with the Centre for the Study of Democracy of the Russian finncial footprint across the region, as well as investigating the relationships between Sputnik and local media outlets.

Raskrinkavanje sees fact-checking media accuracy as a specialism which they publish and promote to the public.

The Center for Study of Democracy and the Center for Euro-Atlantic Studies are not active in this space.

1.3.3 MAPPING OF SOURCES AND NETWORKS

Bulgaria Analytica feels that mapping sources and networks is at the heart of what they do, and they publish regularly on exposing networks. "In exposing Russian propaganda you are fighting a ghost. If you approach counter disinformation without exposing the networks you will fail."

The Center for the Study of Democracy would like to enter into this space but are at the beginnings. They have taken some initial steps toward this with the mapping of media ownership and management, but are seeking to use more sophisticated methodologies and would seek capacity-building here.

HSSF is strongly geared toward this. They are working on charting the network of media outlets engaged in propaganda and naming the particular journalists responsible.

The Center for Euro-Atlantic Studies is strong in this area and has undertaken a recent large-scale project called "Eyes Wide Shut" exposing how propagandist networks operate.

European Western Balkans has strong capacity in this area having recently done a project in conjunction with the Centre for the Study of Democracy of the Russian financial footprint across the region. They have also investigated the relationship of Sputnik with many companies.

Raskrinkavanje manually focuses on following individual stories. This process often takes a few weeks.

ANNEX E: REGIONAL REPORTS

1.3.4 INCREASING PUBLIC AWARENESS OF DISINFORMATION

Bulgaria Analytica uses a number of different methods to raise public awareness of disinformation, including press conferences and strategic briefings with journalists and experts. They work with several journalistic outlets that publish all their work, such as Faktor Bulgaria. They are active across all social media platforms, and also on decentralised platforms like Steemit.

The Center for Study of Democracy sees this as a key component of its duties. They produce fact-based analysis and then use it to raise public awareness of their research.

HSSF is strong in this area. When they published their first report last year, nobody was prepared to recognise there was a problem with Russian propaganda in Bulgaria; now it is used as a set text. They are well-known to Bulgarian media and consulted frequently.

The Center for Euro-Atlantic Studies is engaged here but faces great difficulties given the Serbian media ecosystem.

European Western Balkans, on the other hand, is strong here. There is not a single major news outlet in Serbia that has not published an article by them, including Sputnik.

Raskrinkavanje is actively engaged in this area. It runs a system in which every publication that produces a deliberate inaccuracy is placed on its 'Red List' which is publicised on its website.

1.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

Given the 'dual-threat' environment within which all the organisations above operate, their work is to be commended. The most common strength, and critically one that is backed up with hard evidence, is the capacity to conduct research projects, with almost all organisations having reports available to read on their websites. Conversely, at times, certain claims, especially from Bulgaria Analtyica, lacked substantive evidence.

Fact-checking, as is common across the regions under consideration, was less of a focus, though it is worth noting that Raskrinkavanje and European Western Balkans consider it an important area with which to engage.

The biggest weakness among all organisations was the ability to engage with vulnerable audiences (defined as those most susceptible to Russian propaganda).

1.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

1.5.1 ETHICAL JOURNALISM

As most organisations were think tanks, they did not directly engage with ethical journalism practises as defined by Poynter (most were, for example, unaware of its Fact-Checking Code of Principles). Journalists they engaged with or employed for projects worked according to what they tended to describe as 'general Western standards' of journalism, a vague term.

ANNEX E: REGIONAL REPORTS

1.5.2 DIGITAL COMMUNICATIONS

All the organisations interviewed lack capacity in big data science and social media listening tools. Most are keen to learn and Bulgaria, as a country, has the human capital to enable to these organisations to strengthen in this area if given adequate support.

All organisations suffered limitations due to human and financial resource constraints.

1.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

In Bulgaria the primary cross-cutting issues were the following:

A. **The decline of Europe;** narratives include: 'the refugee crisis is organised by the US and the CIA'; 'hordes are invading to destroy Europe'; 'liberalism is a disease and Europe is sick from it'; 'Brussels institutions are puppets of foreign interests, corporations, Soros etc'; 'Brussels bureaucracy oppresses European peoples'.

B. **Pure conspiracy;** narratives identify the US and NATO (or Wall Street, or the Clintons, or the Rothschilds, etc) as puppet master hegemons. Narratives are often heavily but not explicitly anti-Semitic.

In Serbia, the major narrative is about the sophistication of Russian weapons as a symbol of Russian power. The great popular myth now is that if Russia had had S300 miisies to give Serbia in 1999, it would never have been bombed. Sputnik is one of two websites in Serbia that has a special section on weapons, and it has made the population very interested in Russian weapons, and how they are superior to Western weaponry. A related narrative is that the only reason the West could bomb and destroy Yugoslavia is that Russia was led by the drunk Yeltsin, if Putin had been in power if would never have happened.

1.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

There are two clear fields of upskilling potential: big data capabilities and a need for greater financial and human resources. The competency is there but the resources are lacking.

2. BALTICS

2.1. SUMMARY OF FINDINGS

The Baltic states have been the primary target of Kremlin disinformation in Europe since their independence in 1991. As such, Estonian, Latvian and Lithuanian organisations have unparalleled understanding of disinformation efforts and over the course of the past 20 years have developed considerable resilience to the Kremlin's information campaigns. The resilience, however, does not extend across all clusters of society and is still lacking among native Russian speakers in the Baltic states.

ANNEX E: REGIONAL REPORTS

Baltic organisations working in this space excel at research, network mapping, fact-checking and public outreach, but do not have enough financial resources to scale their activities further. What is notable in the Baltics is organisations' willingness to work together to counter the threat. More could be done, however, with additional training on grant proposal writing, digital communication and cyber security.

2.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

The disinformation threat faced by the region varies across the countries and their different demographic and linguistic groups. Kremlin disinformation targets native Russian speakers, especially those living in Latvia and Estonia. The most common targets of Kremlin-funded disinformation campaigns are national governments, NATO, the EU, Western values and national history.

Most disinformation is spread by Kremlin-funded media outlets operating in the Baltic states, such as Sputnik News, BaltNews, Vesti.lv and others. Social media, especially VK (Vkontakte), has been instrumental in the spread of disinformation in the Baltics.

2.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

2.2.1 DEVELOPING RESEARCH PRODUCTS

Latvian think tank the Centre for East European Policy Studies (CEEPS) does short and long-term research focusing on Russia's influence in the Baltic region. Their research products are very diverse and include long-form research reports, disinformation overviews, studies, books and academic articles. Their main focus in the area of disinformation is on hostile narratives and their development over time.

Estonian think-tank the International Centre for Defence and Security (ICDS) has a dedicated research program for disinformation, which produces analysis of disinformation campaigns. Their research focuses on unpacking the Kremlin's toolkit and looking at some of the ways disinformation is created, spread and consumed.

2.2.2 FACT-CHECKING

Delfi is the largest fact-checker in Lithunaian. It runs a debunking project called "Demaskuok" (in English 'Uncover'). Delfi asks their readers to submit stories that they think might be inaccurate for Delfi journalists to fact-check. They publish debunked stories on their website, which is one of the most visited in Lithuania.

'Lithuanian Elves' are volunteers on social media, who identify disinformation on social networks, fact-check misleading statements and comments, and report them if they are in violation of social networks' community rules. Apart from that, the Lithuanian Elves also take part in Delfi's project where they scan the disinformation monitoring platform that Delfi built and flag content they think might be false or misleading.

ANNEX E: REGIONAL REPORTS

CEEPS partners with Delfi's Latvian outlet on a fact-checking project, where CEEPS produces monthly overviews of main disinformation narratives and debunks 'fake news' in Latvian and Russian. This overview is published by Delfi.

2.2.3 MAPPING OF SOURCES AND NETWORKS

Delfi is leading the way in mapping disinformation sources and social media networks. With funding from Google's Digital News Initiative, Delfi built a prototype for a web-based Artificial Intelligence (AI) tool that currently tracks articles of over 100 websites in Lithuanian and Russian that are known to spread disinformation. The tool can classify articles published by these websites by popularity, keywords, topics, social media shares, author and the countries mentioned.

The 'Latvian Elves', who have adopted a similar methodology to their Lithuanian counterparts, centre their activities around disinformation network mapping. They are currently compiling a list of Facebook accounts and media outlets that spread pro-Kremlin disinformation in Latvia. They want to make the list publicly available to improve the Latvian public's understanding of disinformation.

2.2.4 INCREASING PUBLIC AWARENESS OF DISINFORMATION

Laisves TV is a Lithuanian online television channel that produces video programming available on YouTube, Current Time TV and NTV+ in Estonia. Laisves produces a program in Russian called 'Dherzhytes Tam' ('Hold on there'). It is a humorous night-time show, similar to John Oliver's Last Week Tonight. The shows unpack Russian officials' statements and Russia's foreign policy, military activities and disinformation. The shows are watched by approximately 60,000 people every week across the three platforms.

Apart from Laisves TV, there are very few organisations in the Baltic states that are reaching the most vulnerable communities, namely native Russian speakers. The National Centre for Defence and Security Awareness (NCDASA) is one of very few organisations that do so not only online but also offline. NCDASA organises public events, such as seminars for schoolchildren, training courses for young experts on information and cyber 'hygiene', visits to military units, excursions, shadowing days, open debates, school conferences, as well as meetings with representatives of the political elite, community leaders, experts, government officials, and army officers. They also run courses for mid-level managers, representatives of municipalities, and entrepreneurs where they explain how Estonian defence and security structures work. Their main task is to demystify the defence and security services and make them more attractive for Russian-speaking Estonian citizens.

NCDASA has also run social media campaigns for Estonian Russian speakers. One such example was the #WeAreNATO campaign, which NCDASA ran in Russian for the Russian-speaking citizens in Estonia, under the brand #НАТОэтоМЫ. They used the hashtag to promote NATO and raise awareness about the alliance's history and its Enhanced Forward Presence in the Baltics.

ANNEX E: REGIONAL REPORTS

2.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

The activities listed above had high degrees of success among their respective audiences. Both ICDS and CEEPS have strong relations with the Estonian and Latvian governments respectively, which means their research is widely read by the countries' policy-makers, which helps build their resilience and deepen their understanding of the problem of disinformation.

The success of the two mapping exercises cannot be measured at this stage, as neither Delfi nor the Latvian Elves have made any of their findings public yet. Delfi did confirm, however, that their tool has helped them identify several inaccurate stories that could be classified as Kremlin disinformation, which they then debunked.

The fact-checking efforts by Delfi have been highly effective. Delfi observed that the debunking stories garnered more reads and engagements most of their other reporting, indicating a large appetite for fact-checking content in Lithuania. Neither CEEPS nor the Lithuanian Elves could quantify their impact in this area.

Both Laisves TV and NCDASA have reported high level of success of their outreach campaigns. As mentioned above, Laisves TV's shows in Russian are watched by approximately 60,000 people every week across their three platforms, making them the most influential Russian language channel in Lithuania. NCDASA did not have any relevant metrics for their people-to-people engagement, but their #WeAreNATO campaign in Russian did generate a significant degree of engagement.

2.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

The Baltic organisations interviewed did not have any glaring skills gaps. Most have been active for at least five years, during which time they have developed ethical journalism, research, network mapping and cross-sector research building skills. One competency that some organisations do lack, especially the two think tanks (CEEPS and ICDS), is digital communications. This, however, is not a skill gap, but rather a financial issue as neither CEEPS nor ICDS can afford to hire any full-time digital communications staff.

Although digital communications training could help upskill the employees these organisations already have, a more sustainable way to address this challenge would require some comprehensive training on business models and grant application skills. Very few organisations have experience writing funding proposals and many do not know about the existing funding opportunities available in their region or across Europe more widely.

2.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

One of the most cross-cutting issues in the Baltics is history, which is often used by the Kremlin to deny the legitimacy of the Baltic states' sovereignty, undermine the reputations of their national heroes, and rehabilitate the Soviet period.

ANNEX E: REGIONAL REPORTS

2.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

Out of seven organisations interviewed, two, Laisves TV and the Lithuanian Elves, could greatly benefit from training on social media monitoring. Both organisations want to use social media listening and monitoring tools to understand audiences beyond their own echo chambers and reach vulnerable communities online.

The Lithuanian and Latvian Elves admitted to having cyber security vulnerabilities, which is especially alarming considering both groups have already experienced cyber and social media attacks. The Lithuanian Elves suffered DoS attacks on their servers and some Latvian Elves have been doxed.

Three organisations – ICDS, CEEPS and the Latvian Elves – could greatly upscale their impact with stronger digital communication skills. Think tanks like ICDS and CEEPS are keen on translating their research into more engaging content for social media, whereas the Latvian Elves want to improve their digital communication skills to better counter pro-Kremlin disinformation on social networks.

ICDS and NCDASA expressed interest in improving their grant application skills to make their funding models more sustainable in the long term. Lastly, Delfi expressed interest in cooperating with other organisations working in this space, especially those that could benefit from the AI media monitoring tool they have built, as they are very keen on scaling it.

3. CAUCASUS

3.1. SUMMARY OF FINDINGS

Given their geographical proximity to Russia, the Caucasus states occupy a vital space in the network. Georgia which has experienced recent Russian military aggression, is a particular target of disinformation from Russia, which backs the indepdendence of the separatist territories of South Ossetia and Abkhazia.

The findings here are limited to Georgia at the present time.

The two organisations interviewed, MDF and GRASS FactCheck, were both highly cognizant of the disinformation threat and were particularly strong in fact-checking, making them distinctive among the organisations interviewed across Eastern Europe, the Balkans and the Caucasus.

All organisations expressed great interest in capacity building. Again, increased big data and social media capabilities topped the list.

As with every organisation interviewed, human and financial constraints were a primary obstacle to more effective performance.

ANNEX E: REGIONAL REPORTS

3.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

Unsurprisngly, given its recent history, Georgia is highly Russophobic. Pro-Kremlin disinformation in Georgia is spread not by Sputnik or RT but by Georgian NGOs and journalists. As with the Balkans, Russian propaganda is smuggled into the national consciousness in the form of anti-EU and anti-Western narratives. Public support for Russia is unpalatable to the population, so ultra-nationalistic narratives, which serve the same ultimate strategic goals, are used instead.

As such, the pro-Russia actors in Georgia are internal and deceptive, supported covertly from the Kremlin, and therefore that much harder to combat. While pursuing the broader strategic objective of pulling the country away from Europe and into Russia's orbit, they attempt to convince the populace that they, and not the Russia-sceptic Georgian mainstream, represent true Georgian patriotism.

3.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

3.3.1 DEVELOPING RESEARCH PRODUCTS

MDF has evidence of being strong in the development of research products. They have just produced their annual report 'Anti-Western Propaganda,' which is rigorous and powerful. In terms of methodology, they study the sources of information and the methods used by propagandists. They monitor not only media outlets but also politicians and related financial issues.

GRASS FactCheck conducts in-depth research on disinformation. In 2014, they produced the major report "Myths and Realities on EU in Eastern Partnership Countries." They try to identify the weak spots that the Kremlin seeks to exploit.

3.3.2 FACT-CHECKING

MDF considers fact-checking a speciality. They fact-check and debunk disinformation through their website (www.mythdetector.ge/en) and have partnered with EU's East StratCom Task Force, who have published MDF's content on their website. From summer 2018 they will enter into a new, as yet undetermined form of cooperation.

GRASS FactCheck introduced fact-checking into Georgia in 2013 and are a member of the International Fact-Checking Network at Poynter and a signatory to its code of principles. They grade politicians' statements on a scale of truthfulness, fact-check news reports, and publicise manipulative propagandist narratives.

3.3.3 MAPPING OF SOURCES AND NETWORKS

MDF tries to engage in this area but is constrained by human and financial resources. They are expecting some funding from the Dutch Embassy for a schools programme.

GRASS FactCheck is not as focused on this aspect of counter-disinformation. They rely primarily on work done by other experts in the field, though they seek to update and improve on that work in their own reports.

ANNEX E: REGIONAL REPORTS

3.3.4 INCREASING PUBLIC AWARENESS OF DISINFORMATION

MDF needs capacity here. They previously received funding to produce TV news reports but that has ceased.

GRASS FactCheck undertakes awareness campaigns targeting students and civil society representatives, who are big multipliers when it comes to spreading counter-disinformation. They also offer training on media literacy and fact-checking.

3.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

The organisations are at a severe disadvantage as they are battling television, which is the primary means of spreading disinformation. Whoever controls television in the region controls public opinion. Social media, especially in rural areas, and especially among the elderly, is simply not a factor.

Conversely, given the high anti-Russian sentiment in the country, there is a space for pro-Western voices, especially on independent TV stations. It is necessary to increase capacity to allow for this to happen on a larger scale.

The organisations still face problems in successfully connecting with vulnerable communities. There are sizeable Armenian and Azeri minorities who, unable to understand Georgian television, are a prime audience for Russian television, which often comes packaged with entertaining content, a feature of the most successful Kremlin propaganda. Georgian Public Broadcasting, the country's national public broadcaster, refuses to broadcast in Russian and local minority languages. As a result, these minorities are the least supportive of Georgia's integration with the West.

3.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

3.5.1 RESEARCH

The ability to adequately map disinformation networks was noticeably lacking. The counter-disinformation space as a whole is slightly less evolved than in other regions, still being largely though not exclusively focused on fact-checking, which might be termed counter-disinformation 1.0.

3.5.2 DIGITAL COMMUNICATIONS

All the organisations interviewed lack capacity in big data science and social media listening tools. All organisations suffered limitations due to human financial resource constraints.

3.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

CCross-cutting narratives include (1) that the West will use LGBT rights to impose homosexuality and subvert Orthodoxy; (2) that George Soros is trying to undermine the nation;

and (3) that migrants are a national security threat (this latter narrative became prominent in 2017 with the emergence of the Georgian March, a far-right social movement, some of whose members were arrested for attacking journalists). More recently, The Alliance of Patriots of Georgia, a far-right political party, has made the argument that Turkey poses a greater threat to Georgia's territorial integrity than Russia.

Again, the focus is not necessarily to create pro-Russian narratives but rather anti-Western or, in this case, anti-Turkish ones.

Conspiracy theories are also widespread. For example, a prominent narrative has been that the Lugar Center, a biological research laboratory in Tbilisi built with US assistance, is developing viruses to destroy Georgian genes.

3.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

There is a clear need for greater big data capabilities and a need for greater financial and human resources. Improved capacity to map propaganda networks is also needed.

4. CENTRAL EUROPE

4.1. SUMMARY OF FINDINGS

Central European countries are an important target of the Kremlin's disinformation campaigns. Poland, the Czech Republic, Slovakia and Hungary have all built up some resilience in the past couple of years, but are still behind the Baltics in terms of the societal awareness of the threat that Kremlin disinformation poses to the region and to individual countries.

The eleven organisations interviewed were all well aware of the disinformation threat and excelled at research, network mapping and public outreach. Not a single organisation, however, focused on fact-checking, with only one Hungarian think tank, Political Capital, highlighting fact-checking as an important tactic.

All organisations interviewed expressed their interest in capacity building, especially training on social media research, big data analysis and digital communication, as well as training on grant proposal writing and sustainable business models.

4.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

The disinformation threat faced by the Central European countries is highly complex and closely interlinked with domestic power dynamics and local fringe groups. Kremlin disinformation efforts are increasingly focused on amplifying and appealing to the growing far left and far right communities in the 'Visegrád four'.

Domestic pro-Kremlin governments, especially in the case of the Czech Republic and Hungary, add a new layer of complexity to this mix, making disinformation both an internal and an external threat.

ANNEX E: REGIONAL REPORTS

4.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

4.3.1 DEVELOPING RESEARCH PRODUCTS

Czech think tank European Values runs the Kremlin Watch programme, which aims to expose and confront instruments of Russian influence and disinformation operations focused against Western democracies. As part of the programme, European Values puts out a weekly newsletter summarising recent events relating to Kremlin disinformation that gets sent out to more than 5,000 journalists, NGO workers, government officials and members of the public.

Hungarian think tank Political Capital monitors Hungarian state media and Hungarian-language pro-Kremlin media outlets, including fringe media sites that push far-right conspiracy theories. They publish reports on a variety of disinformation-related issues, primarily focusing on how Russia is utilising far-right groups across Hungary and the region.

The Prague Security Studies Institute (PSSI) analyses disinformation in relation to certain events such as elections. They have built up strong capabilities in this area over the last two Czech elections (notably with a project titled 'Czech Elections in the Era of Disinformation') and tend to study disinformation's broader social and public effects.

Warsaw-based think tank the Center for European Policy Analysis (CEPA) has been researching propaganda and disinformation for over three years. In 2016 they launched the StratCom Program, the goal of which is to analyse the dissemination of pro-Kremlin narratives in Central and Eastern Europe. As part of the project, they are looking at techniques that are used to spread disinformation and target vulnerable groups as well as the way disinformation reaches its audiences.

The Polish Center for International Relations (Centrum Stosunków Międzynarodowych, CSM) focuses on long-term research products tracking pro-Kremlin narratives in Poland, as well as the broader region. CSM analyses and raises awareness about Russia's influence activities to disrupt democratic transitions in Central Europe and undermine European unity. Together with partners from other Visegrad countries, the PSSI conducted an in-depth country monitoring survey and examined the variety of influence measures that were being leveraged by the Kremlin.

Slovakian think tank GLOBSEC carries out unique research on public perceptions of and reactions to Russian narratives and conspiracy theories within the region. The think tank publishes the annual GLOBSEC Trends report, which covers Eastern and Central Europe and analyses public opinion on various issues including East-West relations, the EU, Russia, NATO, and media consumption.

In partnership with the International Republican Institute (IRI), the Polish Center for Propaganda and Disinformation Analysis (CAPD) monitors the Polish media environment, both online and offline, to identify any Russian narratives that are penetrating the media ecosystem and dominant messages and vulnerabilities.

4.3.2 MAPPING OF SOURCES AND NETWORKS

Slovakian think tank the Institute for Public Affairs has mapped members of the pro-Russian community and Russian organisations influencing the public debate in Slovakia.

ANNEX E: REGIONAL REPORTS

4.3.3 INCREASING PUBLIC AWARENESS OF DISINFORMATION

Poland's Kosciuszko Institute organises the annual CYBERSEC Forum, which brings together businesses, policymakers, academics, NGOs and influencers to foster the building of an Europe-wide cybersecurity system and to create a dedicated, collaborative platform for governments, international organisations and key private sector companies. Disinformation is a small subset of the cybersecurity recommendations document that they release every year, but in the future they intend to expand their work in this area. They are keen to take on the role of a network convener and are interested in developing recommendations on how governments can build counter-measures and increase resilience to disinformation.

Polish media outlet Defence24 is the biggest new portal on defence-related issues in Poland. They publish articles related to disinformation and information security that reach thousands of readers.

Based on their public opinion surveys, GLOBSEC carried out an online campaign using social media influencers to illustrate the risks posed by disinformation, which achieved 1.2 million views in a country of 5 million people (though there was some spillover into the Czech Republic). GLOBSEC assessed it as the most successful ever counter-disinformation campaign in the region. They carry out public discussions for young people at music festivals where they have also run interactive workshops, as well as setting up an e-learning portal for NGOs and civil society organisations that want to carry out activities in this area, with guidelines, how-to manuals, and links to online resources.

Slovak media monitoring organisation Memo 98 is increasing public awareness of disinformation by monitoring Russian media and exposing misleading reporting. They have plans to produce social media content for Russians living in Russia.

CAPD are working with GLOBSEC on a project to counter disinformation in the V4 countries. As part of that, in summer 2018 they will run a small public awareness campaign targeting university students to inform them about the threat of Russian disinformation in Poland. It will be the country's first public campaign on the subject of disinformation.

4.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

The activities listed above have had varied degrees of success among their respective audiences, but it is noteworthy that some organisations struggled to back up statements on their impact with hard data.

The research outputs produced by European Values, Political Capital, PSSI, CEPA, CSM, GLOBSEC and CAPD have managed to reach their target audiences, which consist of national and regional decision-makers and policymakers. However, an understanding of the threat that Kremlin disinformation poses does not appear to have entered the public discourse.

Out of eleven Central European organisations interviewed, only one, GLOBSEC, is successfully reaching considerable audiences in a Central European country, with the remaining ten organisations lagging behind.

None of the eleven organisations interviewed appear to be successfully reaching the most vulnerable communities: avid consumers of Kremlin disinformation.

ANNEX E: REGIONAL REPORTS

4.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

The Central European organisations interviewed had some skills gaps in digital communications and research. It appears that most of the organisations have now done plenty of research to understand the Kremlin's disinformation efforts and are ready to proactively engage with the threat through public outreach. Three organisations, the Kosciuszko Institute, Defence24 and Political Capital, require some more serious upskilling.

As in other regions, most organisations interviewed require comprehensive training on sustainable business models and grant application skills. Not all organisations have experience writing funding proposals and many do not know about the existing funding opportunities available in their region or across Europe more widely.

4.5.1 RESEARCH

The Kosciuszko Institute and Defence24 have very limited skills when it comes to researching disinformation and both organisations expressed an interest in developing these competencies. Political Capital is very keen on developing their fact-checking capacity, as there are very few fact-checking organisations in Hungary, and investigative reporting as an output is not immediate enough to counter the country's growing disinformation problem.

4.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

In the Czech Republic, the two cross-cutting issues were negative attitudes towards migration, especially from Muslim countries, and negative sentiment towards the European Union, which is exploited not only by the Kremlin, but also by far-right groups.

A similar pattern was also observed in Hungary, where Kremlin disinformation spreads far-right narratives as they relate to migration, liberalism and the EU.

Slovakia and Poland were not affected by this as much. Instead, Kremlin disinformation targeted the relationship between Poland and Ukraine, and in Slovakia, it exploited the narrative of Russia as a Slavic 'big brother', highlighting the historical ties between the two countries.

4.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

Overall, most organisations interviewed lack digital competencies, namely digital research and digital communications skills.

Out of eleven organisations interviewed in the region, four (PSSI, Political Capital, CEPA and GLOBSEC) could greatly benefit from training on big data and social media listening tools, which could add a new dimension to their research products. Another five organisations, namely Memo 98, Defence24, CAPD, CSM and CEPA require training in digital communication and outreach, which would help them connect with new audiences.

Apart from that, Political Capital requires fact-checking training and European Values relayed the need for more Russian language capabilities within the team.

Most organisations in the region highlighted the need for greater financial and human resources.

ANNEX E: REGIONAL REPORTS

5. EASTERN EUROPE

5.1. SUMMARY OF FINDINGS

The Eastern European region is comprised of countries that are on the frontline of the Russian disinformation war. The organisations under consideration in this region – StopFake, Detektor Media, the Association of Independent Press (API), ZDG, Newsmaker, Euroradio, and the Belarusian Association of Journalists (BAJ) – come from three countries, Ukraine, Moldova and Belarus, which were all part of the former USSR.

Ukraine remains at war with Russia in all but name following the Kremlin's annexation of Crimea in 2014 and subsequent military incursion into the country's East to help form and encourage a separatist movement there. Ukraine was the laboratory for much of the hybrid disinformation operations that Russia has used since. Belarus and Moldova are subsumed almost entirely within Russia's 'sphere of influence', though the relationship with Belarus is slightly more complex. Accordingly, this is arguably the most vital space in the entire Network.

All organisations were highly cognizant of the Russian threat and, given its intensity, were highly proactive, often in the face of significant obstacles. All expressed an eagerness to be part of the Network and were receptive to capacity building across all areas.

5.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

There is considerable variation among the countries within the region. Ukrainian organisations StopFake and Detektor Media, working in a country in a state of war with Russia, therefore carry out their work with full government support and backing. The Moldovan organisations API, ZDG and Newsmaker are effectively investigative journalism outfits that are working within a dual-threat environment. The situation is even more severe in Belarus, often referred to as 'the last dictatorship in Europe', where Euroradio is forced to work from Poland and most independent journalists have spent much of their careers underground, though the situation has improved recently.

Ukraine is facing an all-out disinformation war from the Kremlin. According to StopFake there are 18 main narratives used. Each is effective in its own way and for different audiences. For example, the narrative that Ukrainians are fascists and attacking the Ukrainian army does not work in Ukraine proper, but is successful in the occupied territories. Now the most prominent Russian narrative centres on Ukraine being a failed state.

However, organisations receive strong support from the government and work closely with the relevant government ministries in combating Russian disinformation narratives. The banning of Russian TV in the country has helped with counter-disinformation efforts, and within Ukraine proper, Russian narratives gain little traction. The problem remains with vulnerable communities in the occupied East.

In Belarus, Russia exerts various forms of pressure on the government. Russia has traditionally been the chief export market for Belarusian foodstuffs, so it applies political pressure on Belarus' president Lukashenko through intermittent bans on Belarusian imports on various pretexts; a common one is that hazardous substances have been found in food. Accordingly, while Russia ultimately dominates Belarus, the relationship between the two countries is, to a degree, ambivalent. After the EU imposed sanctions on Russia following the annexation of

Crimea, which caused Russia to sanction EU imports in return, Belarus took the opportunity to buy from countries like Poland and sell to Russia at a profit. As such, in the disinformation sphere, Russian narratives are both positive and negative, focusing, on the one hand, on Belarus as an unreliable partner and, on the other, stressing pan-Slavism: that Russians, Belarusians and Ukrainians are one great people.

Organisations in Moldova operate in a severe dual-threat environment. Russia's access to Moldovan domestic politics is its biggest source of strength in the country. The Moldovan government claims to be pro-European, but the statements and actions of its president and prime minister indicate a strong affinity with the Kremlin. Chisinau has paid lip service to the West by, for example, enacting an anti-disinformation law to ban propagandist outlets, but it has simultaneously placated Russia by excluding a number of Russian TV stations from the ban.

5.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

5.3.1 DEVELOPING RESEARCH PRODUCTS

StopFake carries out at least two major research campaigns each year, in Ukraine and externally with its international partners. Its founder, Yevhen Fedchenko, is director of the Mohyla School of Journalism and head of their PhD programme in mass communication, of which countering disinformation is a major competent. StopFake partnered with the Reuters Institute on a project looking at bots and trolls in the Ukrainian internet. It is highly competent in this area.

Detektor Media has run qualitative and quantitative studies on subjects such as the quality of journalism in Ukraine.

API is not presently occupied with developing research products, though they are interested and would be keen on greater capacity here.

ZDG and Newsmaker are investigative journalism outfits, both of which produce detailed reports and projects, though not about Russian disinformation per se. They are weak in this space but the capacity is there, if properly directed.

Euroradio is lacking in this area but is interested in entering the space were it possible to upgrade their capacity. They have carried out long-term investigative research on local issues, but not on Russian disinformation.

Two years ago, the BAJ presented a detailed and wide-ranging proposal to the Belarusian government to reform the country's media in the interests of resisting Russian disinformation, indicating that they are strong in this issue.

5.3.2 FACT-CHECKING

StopFake began as a fact-checking outfit and continues to work in this space. It is presently hiring more fact-checkers and foresees that this will continue.

Detektor Media is strong in this area. It is both a think tank and a media outlet, and its articles exposing Russian disinformation are disseminated widely in Ukraine, including to government officials and media partners.

API is well-known for debunking fake news, and has a reputation for objectivity and political independence. They organise training events for fact-checkers, which is especially important in Moldova where disinformation is so prevalent.

ZDG and Newsmaker carry out fact-checking as a de facto part of their journalism, as does Euroradio, which maintains a section on its website called 'fact check', where they verify statements made by Lukashenko and Putin.

BAJ is not engaged with fact-checking as they consider its value and its interest to the public to be limited. They believe that successful counter-disinformation needs to be well-packaged.

5.3.3 MAPPING OF SOURCES AND NETWORKS

StopFake produces stories about networks whch it feeds to other media. It tries to work with whistleblowers from inside the system, for example, ex-RT host Liz Wahl, and publishes their testimony.

Detektor Media and Newsmaker are not active in this area.

API and Euroradio are engaged to a limited degree. Both, especially Euroradio, are interested in doing more, but both would need greater capacity, as they face resource constraints and a lack of training.

ZDG carries out activities in this area as a de facto part of its journalism.

BAJ produced a major report mapping Russian propaganda networks in 2014 in association with six organisations in other countries. They continue to monitor this space.

5.3.4 INCREASING PUBLIC AWARENESS OF DISINFORMATION

StopFake uses its media platforms to engage with the public, but also runs outreach programmes across the globe in the form of workshops, lectures, conferences, and media training.

Detektor Media raises public awareness of disinformation through their journalistic output and their monitoring activities. Once a month their experts produce a report on the standards of journalism on Ukrainian TV. Their reports are also disseminated, often in a simplified form, to local media throughout the country.

API is considered to have strong capacity in this space across Moldova. They give Moldovan citizens the capacity to report fake news online or through an app. They have recently

received a grant from the European Commission that will allow them to hire and train a network of 35 part-time staff across the country, comprising journalists and activists who enjoy credibility with local populations. The project started in April and will last for 20 months.

ZDG, Newsmaker and BAJ engage with this issue as a de facto part of their journalistic work, as does Euroradio, which considers raising public awareness of disinformation to be at the heart of what it does.

5.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

Quality of activties varies greatly across this region. It is clear that Ukraine is the most effective in combating Kremlin disinformation while both Moldova and Belarus suffer from serious internal, governmental threats, combined with a severe lack of human and financial resources.

However, perhaps counter-intuitively given the gravity of the threats faced, organisations here were unusually well skilled in engaging with vulnerable audiences. Detektor Media has run projects in occupied East Ukraine, questioning people about their thoughts on the Ukrainian press, how they consume media, and the conflict itself. Their report concluded that those living in the occupied areas have far less access to objective information and instead favour mass consumption of Russian media.

API runs a project to train journalists and activists across Moldova, focusing on rural areas where the populace is most susceptible to Kremlin disinformation.

Critically, both Ukrainian and Belarusian organisations understood the need to package counter-disinformation in an entertaining format.

5.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

5.5.1 ETHICAL JOURNALISM

Apart from StopFake, none of the organsiations were familiar with the Poynter fact-checking code of principles.

5.5.2 DIGITAL COMMUNICATIONS

All the organisations interviewed lack capacity in big data science and social media listening tools. All organisations suffered limitations due to human and financial resource constraints.

ANNEX E: REGIONAL REPORTS

5.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

In Ukraine and Belarus, Russian TV has recently started to move its most egregious propaganda narratives from its largely discredited news organisations to talk shows, again combining news with entertainment. American and Ukrainian guests, often chosen for their odd appearance, are introduced as “experts” for “balance”, and then humiliated by their pro-Russian interlocutors before a clapping audience. Inter, a pro-Kremlin channel which is owned jointly by the oligarch Dmytro Firtash and Channel One Russia, is the third most-viewed in Ukraine.

In Moldova, major anti-West narratives relate to what will happen if Moldova joins the EU: (1) that churches will be closed and Christian burials forbidden; (2) that people will be forced to embrace LGBT rights; (3) that the slaughter of animals and the cultivation of cucumbers will be banned under EU farming laws; (4) that Moldovans will lose their culture; and (5) that the EU will instigate war with Russia.

As with all Russian narratives, where overtly pro-Kremlin lines cannot be used, as in, for example, Ukraine, the goal instead is to undermine the West, specifically the EU, the US and NATO.

5.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

There is a clear need for greater big data capabilities and a need for greater financial and human resources. Greater capacity to map propaganda networks is also needed.

ANNEX E: REGIONAL REPORTS

6. SOUTHERN EUROPE

6.1. SUMMARY OF FINDINGS

We found that the number of organisations specifically focused on disinformation in Europe was relatively small. In Italy there are two organisations that work effectively in the area. These are Fanpage.it, which does not have a specific focus on disinformation, but which has done some work with DFRLab in that area, and Pagella Politica. Pagella Politica is a very competent organisation that does comprehensive fact checking, but it focuses mainly on statements made by Italian politicians.

There is a dearth of organisations working on tackling disinformation in Spain. Only one organisation is dedicated to debunking falsehoods: Maldito Bulo. There are think tanks that have some research capability relating to Russian sisinformation. CIDOB has done very good work in this area, but only has one researcher that focuses on the topic.

Organisations expressed some frustration at governments' slow response to the threat posed by disinformation. The Spanish organisations have noted that the Spanish government has shown a reluctance to talk to them about disinformation, although CIDOB does have some government contacts. It appears that the Spanish government is reacting piecemeal to specific incidents, for example the Catalonia crisis. Moreover, its focus appears to be technical in nature. Their response has been in the cyber domain and is based on protecting Spanish infrastructure. It has not done enough, in the views of our interviewees, to tackle the possible impact of disinformation on discourse.

Interviews have shown that while there are not many organisations working in the area, those that are are highly competent in the niches on which they focus. CIDOB provides high-quality research into discourse, which it distributes selectively to private audiences. Maldito Bulo is able to rapidly fact check 'fake news' and debunk it to their audience. There is significant potential to upskill partners and some, in particular Maldito Bulo, have expressed a desire to improve the skills of their volunteers.

6.2 THE THREAT POSED BY DISINFORMATION IN THIS REGION

There is an increasing threat posed by disinformation in this region. As noted by CIDOB's disinformation researcher, the Spanish market is important to Russia because of the language. By creating Spanish-language disinformation, Russia can reach Spanish speaking audiences in Latin America and in the United States. Moreover, as there is no memory of armed conflict between Russia and Spain, the audience may be less reflexively hostile to Russian narratives. It is possible that the Spanish state is reluctant to consider Russian disinformation a national security issue due to Russian investment, tourism and business in Spain, and that therefore it is being ignored.

Disinformation became a significant problem surrounding the Catalan crisis in late 2017. The European Commission Expert Group on Disinformation disagreed over the extent to which Russian involvement was provable. Experts including Jimenez Cruz of Maldito Bulo and Alexios Mantzarlis of IFCN-Poynter were skeptical and hesitant to attribute too much of the blame to Russia. In Italy people are aware that there is disinformation but emphasise that there is no direct evidence of Russian involvement. Some citizens believe that Russian influence is a convenient scare tactic that allows some governments to justify cutting back on information rights.

ANNEX E: REGIONAL REPORTS

The threat manifests itself in different ways. Disinformation spreads easily on Twitter and WhatsApp among the general public. People sharing disinformation through WhatsApp and on private Facebook pages pose the greatest challenge to debunkers as they cannot be engaged with. Russian diplomats attempt to meet policymakers, diplomats, and people in the private sector, so disinformation spreads among elites in a more organic way. Spanish interviewees noted that there is a lot of Russian money in the country, which means that there is resistance to acting against Russia.

6.3 DISINFORMATION PREVENTION ACTIVITES IMPLEMENTED BY PARTNERS IN THE REGION

6.3.1 DEVELOPING RESEARCH PRODUCTS

CIDOB focuses on developing research products. Their disinformation researcher has a big network of contacts in Spain, and in particular in Madrid. He notes that interest in his work has increased substantially in the last two to three years. However, he is more discreet with his disinformation work than with the other issues he works on, which he publishes more widely. He circulates memos and analysis of research relating to disinformation, but privately to specific audiences.

6.3.2 FACT-CHECKING

Maldito Bulo focuses on debunking fake information on social media using images and infographics that are easy to share and read. Currently their work is mainly based on breaking news, but they have expressed awareness that this may not be the best approach and are currently working on a prototype to identify what disinformation is going to go viral.

6.3.3 MAPPING OF SOURCES AND NETWORKS

None of the organisations in this area that were interviewed mapped sources and networks.

6.3.4 INCREASING PUBLIC AWARENESS OF DISINFORMATION

Maldito Bulo's strengths lie in fact-checking and communicating their findings to the public. Additionally, they are working with universities to provide young people with the tools to spot disinformation. They are focused on increasing awareness and public resilience; they produce manuals and video guides to educate the public.

CIDOB's disinformation researcher has indicated that the purpose of his work is not to increase public awareness, and that, as outlined above, he publishes work in this area privately.

6.4 EFFECTIVENESS OF ACTIVITIES IMPLEMENTED BY PARTNERS IN THE REGION

Maldito Bulo is very effective at fact-checking and debunking disinformation. However, they are aware that more research needs to be done in order to gain a better understanding of what can be done to tackle this. Their formula of "No, X does not do Y, it is a hoax" style posts has

been copied by many other media organisations due to the ease with which it is shared. They have 149,000 followers on Twitter; 62,000 on Facebook; and 1,700 on Instagram. It is evident therefore that people are engaging with their content. They are currently focusing on building their Instagram presence in order to reach a younger audience.

It is difficult to know exactly how effective CIDOB's research products on disinformation have been, as they are distributed primarily through private channels. However, the research that CIDOB has done on disinformation has received attention from security services, the private sector and the public sector, who are all now aware of the issue of disinformation to some extent. The think tank has received recognition for its work, and in 2017 was ranked at number 60 globally (and number one in Spain) in the University of Pennsylvania's Global Go To Think Tank annual report.

6.5 SKILLS GAPS IDENTIFIED IN PARTNERS IN THE REGION

6.5.1 ETHICAL JOURNALISM

Maldito Bulo encourages rigorous journalism, but many of their volunteers have not had much formal training. Instead, they fact check each other. They find and source stories through social media, where people send them links to fake news. Once they have received a link, a member of the team writes an article. The rest of the team then ask questions and fact check the fact-checked article. If they cannot clearly identify the source of a story they do not debunk it.

It is worth noting that Maldito Bulo's two founders are experienced journalists who have worked at reputable outlets; they have provided the team with some training in journalistic skills. The founders believe that it is the responsibility of journalists to be aware of media and libel laws at all times, and they are aware of the Poynter fact-checking code of principles. While training could be improved, it seems that this is an area that there are few gaps in.

CIDOB is not a journalistic outfit but its Russian disinformation researcher subscribes to the principle of two-source confirmation.

6.5.2 DIGITAL COMMUNICATIONS

CIDOB does not work on public awareness campaigns or fact checking. Its audience is not the public, or people vulnerable to disinformation, and it does not measure success in terms of audience numbers reached. In fact, CIDOB's disinformation researcher deliberately avoids sharing his research with a large audience because he is aware it might be contentious; he does not tweet most things he does relating to disinformation.

Maldito Bulo creates different formats to convey information on social media in order to increase the amount of people that will engage with it. For example, they debunk fake stories in images so that the final product is easy to share and to read. However, they do not have any staff dedicated to communications or digital media. Instead, everyone chips in where they can. Their current audience is in the 30-50 age bracket; however, they are trying to address their lack of younger readers by building a larger presence on Instagram. They do not have digital tools to understand this audience better, so the younger team members explain Instagram dynamics to older team members. They are currently working on improving their data science capabilities in order to be able to reach the public in a more useful way. They do not have time to develop social media capabilities and do not use any social media listening tools.

6.5.3 CROSS SECTOR RELATIONSHIP BUILDING

CIDOB currently works with the Institute for Statecraft, but they are not comfortable outlining the details of this relationship until they know more about this project. While they do not have any formal arrangement with the public sector, staff have personal relationships that are key to access. CIDOB is not aware of any other local, national or regional networks that are tackling disinformation, except for Maldito Bulo. They express frustration that the Spanish government is not doing more.

Maldito Bulo talks to researchers at universities who research disinformation, but they are currently looking for funding and ways to expand their network. They note that approaches to countering disinformation need to be both hyper-local and Europe-wide. They show a willingness to engage with policymakers but lament that the same policymakers do not engage with them, despite their founder having been part of a high-level European Commission group on disinformation.

6.6 KEY CROSS CUTTING ISSUES THAT IMPACT THE REGION

Italian organisations are doing significant amounts of work tackling corruption.

6.7 POTENTIAL FOR UPSKILLING PARTNERS IN THE REGION

Maldito Bulo appears to be a very capable organisation doing good work, but it is underfunded. It only pays one member of staff and cannot afford technology that would allow it to do its work more effectively. Moreover, they are stretched in terms of volunteer numbers and therefore do not have the capacity to conduct long-term research projects. The organisation would benefit from additional funding to improve their research capabilities and staff numbers.

Maldito Bulo has expressed an interest in additional training. They would benefit from technical training in areas such as data analytics, and some of their younger members might benefit from additional journalistic training. Additionally, they would benefit from learning how to spread their content to a larger, broader audience, as currently their approach is to simply try to grow their Instagram following.

CIDOB is very capable in all the areas they engage with. The main issue is that only one researcher is working on disinformation. There is potential to increase their digital communications capability, although currently this is not something that they are interested in doing with regards to their work on Russian disinformation. The data science capability of the organisation could also be increased.