A Network of NGOs

Technical Proposal

Submitted by:

ZINC
NETWORK

SUBMITTED TO
The UK Foreign & Commonwealth Office (FCO)

NAME OF PROPOSING ORGANISATION/FIRM
ZINC Network

COUNTRY OF REGISTRATION
UK

ADDRESS
Notcutt House, 36 Southwark Bridge Road,
London, SE1 9EU

PHONE
+44 (0) 20 3906 9103

Submitted 31st August 2018

Consortium Partners:

AKTIS STRATEGY

The Institute for Statecraft

bell¿ngcat

MEDIA DIVERSITY INSTITUTE

Digital Forensic Research Lab

TORO

ECORYS

1.1 Executive Summary

State backed disinformation is not just about propagating false or misleading information, but more broadly about manipulating the information environment to further anti-democratic objectives such as undermining the credibility of mainstream media, growing cynicism and distrust towards democratic institutions and processes, increasing polarisation between communities, or destabilising international alliances. The tactics used by the Kremlin and other actors to achieve these ends are adapted depending on the context and objectives and involve not only the dissemination of false narratives, but also the instrumentalisation of wholly or partially true narratives to harness the existing attitudes, beliefs and fears of target audiences, particularly those already disaffected from the 'mainstream'. **To effectively counter disinformation we must therefore deploy a broad suite of approaches by which go beyond fact checking or myth busting, and use audience-centric communications to undermine the credibility of disinformation sources for specific target audiences whilst building their resilience in the long term.**

A growing number of CSOs, activists, academics, policy makers and media organisations are emerging to respond to this threat. While motivated and engaged, they are often working in isolation, responding tactically to a narrow aspect of the threat, and have no way of designing their activities on the basis of real impact. Moreover, they face extensive challenges and threats to their operations which restrict them from reaching their full potential. These include a lack of expertise and tools to deliver high-quality open source research, a lack of ability and support to conceptualise and deliver public facing campaigns that genuinely engage the audiences actually vulnerable to disinformation, a lack of access to grant funding and core resources, and an absence of security frameworks and legal training to run streamlined and low-risk operations in the face of significant threats. **To unleash the capability of these actors to sustainably challenge disinformation requires a joined up, grassroots-led approach which helps organisations to overcome these barriers.**

Bringing together organisations including ZINC Network, the Institute for Statecraft, Aktis Strategy, Bellingcat, DFR Lab, the Media Diversity Institute, Toro Risk Solutions and Ecorys, our Consortium combines recognised market leaders in understanding, monitoring, and countering Kremlin-backed disinformation. Collectively, our experience and skillsets encompass; research and strategy; media development and journalism training; digital communications and behavioural change campaigning; good governance and statecraft; digital forensics research; live tracking and analysing of disinformation; grassroots network management and capacity building; monitoring and evaluation; and policy and research. This is underpinned by extensive experience in risk and financial management and project delivery in complex environments.

The solution we propose will bring together disparate organisations around Europe, training and supporting them across key areas to increase their ability to deliver effective counter-disinformation activities, anchored in research and data. This ecosystem of credible voices will continue to grow, exposing the actors and networks behind Kremlin-backed disinformation, reducing unwitting multipliers of disinformation, and building resilience amongst key target audiences across Europe.

We will mobilise a Network Hub based in London, led by an experienced Project Director, consisting of an agile team with core competencies augmented by a wider pool of vetted experts. Our approach is highly localised, based around regional clusters of actors who can collaborate to effectively undermine the disinformation ecosystem in their respective areas and engage audiences most vulnerable to disinformation. Regional Network Managers – experts in countering disinformation with deep understanding of local dynamics and key stakeholders - will be the primary interface between regional clusters of organisations and the Hub. **Our approach to capacity building includes not only formal training but also intensive mentoring and 'learning through doing', included through embedded mentoring and learning in digital forensics (Bellingcat) and co-created public facing campaigning (ZINC).**

Our approach is based on five pillars: **BUILD > SUSTAIN > TRAIN > CAMPAIGN > SCALE.** Each of these pillars is designed to address a specific gap identified in the scoping research.

- ***Build*** focuses on creating an agile, high impact Network that can effectively counter disinformation in target countries, addresses the lack of coordination between organisations and the isolation they experience by creating groups for knowledge sharing and peer-to-peer support, and connects organisations with the local experts and resources they require;
- ***Sustain*** overcomes the resourcing challenge by providing core funding through a grants mechanism, developing organisational business plans and helping them to access third party funding opportunities, and support to help members to put in place governance structures, operating procedures, risk

management approaches and basic legal and insurance requirements to increase organisational sustainability;

- ***Train*** will ensure members are upskilled and mentored in best practice in exposing and countering disinformation from open source research through to viral video production and digital targeting as well as cyber security, libel and data compliance;
- ***Campaign*** will enable them to increase the pace, scale and quality of their outputs and activities, targeting specific vulnerable audiences through a process of campaign co-creation and project specific funding;
- ***Scale****, which is outside of scope of the ToR, but integral to our network model,* will link the organisations across borders, establish a shared set of standards and protocols and feed learnings up and out to wider stakeholders including policymakers and tech companies.

The approach has been designed with sustainability at its core. Each pillar of our operating model (described in section 1.5) is designed to ensure long-term technical and financial sustainability of project beneficiaries in different ways. **Our approach to sustainability targets three layers; sustainability at the level of the individual organisation, the level of partnerships and cluster building, and also the sector as a whole.**

Underpinning these activities are rigorous monitoring and evaluation, risk management, and quality assurance procedures. In complex, partner-led projects, our experience is that the **risk environment and context is constantly evolving**, which requires close monitoring with flexible strategies adapted accordingly. It is a highly complex project involving coordination of many independent actors, and thus risk must be carefully managed and risk profiles constantly adapted, serving as the basis for all activity. The approach we propose is based on the ***identification, monitoring and management*** of risks as they materialise, allowing members to continue taking smart risks as they increase the scale and impact of their activities. Safeguarding (discussed further in sections 1.2 and 1.3) partner organisations, staff, and project beneficiaries remains paramount to the project and is a core feature of the proposed risk management framework.

1.2 Safeguarding

The safeguarding risks in this project are manifold, and manifest at different stages in project delivery. We understand them as:

- Risks posed by the activity of hostile malign actors
- Risks posed by the behaviour of suppliers

Safeguarding Risks Posed by Hostile Malign Actors

In complex, partner-led projects, our experience is that the **risk environment and context for safeguarding is constantly evolving**, which requires close monitoring with flexible strategies adapted accordingly. The consortium's understanding of partner safeguarding risks and management has been built up over 50 projects with partner organisations, and over 100 individual contributors in Tunisia, Somalia, Iraq, Bangladesh, and across Europe including the Baltics and Eastern Ukraine.

In the context of Kremlin disinformation, we have seen a recent shift in focus from undermining, trolling and doxxing of specific individuals, to the targeting of think-tanks and funders[1]. **Tactics vary greatly depending on the target and which region they operate in**; in North West Europe we observe smear campaigns and online trolling,[2] whereas in Southern Europe and the Balkans proxy media outlets promote separatism and ethnic tensions,[3] and in Syria the White Helmets have been placed under direct physical threats.[4] Safeguarding risks can be long-term, slow-boil irritants, or they can be high-stakes, urgent situations including threats to physical safety or of irreversible damage to sites and systems. The consortium has the experience to know the difference and to calibrate responses. The project has been designed to: (1) ensure a level of training and support to all partners that will work towards their safeguarding, and (2) include a flexible response mechanism that can be implemented in the most critical incidents.

Safeguarding Risks Posed by the Behaviour of Supplier(s) and its Staff

<u>Social Responsibility and Respect for Human Rights</u>
The Consortium will integrate safeguarding measures to ensure that social responsibility and respect for human rights are paramount across all project employees and beneficiaries. This is particularly focused around children and young people and is of paramount importance in light of recent revelations about supply partners working in developing countries. Our safeguarding policy explicitly recognises our moral and statutory responsibility to safeguard and promote the welfare of all children and young people. We endeavour to provide a safe and secure environment where children and young people are respected and valued, and where they can learn and develop, and to safeguard the welfare of all children and young people by taking all reasonable steps to protect them from physical, sexual, or emotional abuse or neglect. We do this by:

- Ensuring all our staff and volunteers are carefully and rigorously selected, trained and monitored, and are supported by a robust safeguarding portfolio
- Carefully assessing all risks that children and young people encounter, and taking all necessary steps to minimise and manage those risks
- Letting parents, children, young people and staff know how to voice concerns or complaints about situations or circumstances they are not happy with

All ZINC staff are required to undertake training modules using our online *CascadeGo* HR system, that includes Safeguarding, Data and GDPR Regulations, and Code of Conduct and Ethics. Our Safeguarding training module includes awareness of modern-day slavery and human rights abuses. ZINC operates employment practices in line with the International Labour Organisation (ILO) 138 convention and Ethical Trading Initiative (ETI) Base

[1] In August 2018 Microsoft identified a Russian government-directed cyber attack on right-leaning American think tanks' websites including The Hudson Institute and IRI. [https://www.hudson.org/research/14510-hudson-institute-statement-on-russian-cyberattacks, https://www.wsj.com/articles/russian-hackers-target-conservative-groups-in-widening-cyberattacks-1534824060]

[2] Bentzen, Naja (2018, July) Foreign influence operations in the EU. European Parliamentary Research Service. [http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf]

[3] Eisentraut, Sophie, and De Leon, Stephanie (2018, March) Propaganda and disinformation in the Western Balkans: how the EU can counter Russia's information war. Facts and Findings: Konrad Adenauer Siftung. [http://www.kas.de/wf/doc/kas_51729-544-2-30.pdf?180306092933]

[4] Lucas, Scott (2018, August 16) The White Helmets and the long history of attacking humanitarians. EA Worldview. [https://eaworldview.com/2018/08/the-white-helmets-and-the-long-history-of-attacking-humanitarians/]

Code, which includes ensuring child labour is never used, statutory minimum age for employment is met, working hours are not excessive (37.5 hours on average), and equal opportunities are provided to all regardless of ethnicity, religion, age, disability, gender, marital status and sexual orientation. We are in the process of signing up to the United Nations Global Compact, and have already begun to enmesh the 10 key principles of human rights, labour, environment and anti-corruption within our Sub Contractor and employee Code of Conduct to ensure that these principles are embedded throughout all of the work that we do. The Project Director will be responsible for ensuring our employee Code of Conduct and environmental, social and human rights policies are adhered to across our countries of operation. We will report any misconduct to the relevant authorities and will investigate all allegations or suspicions of misconduct and take appropriate action (including disciplinary) against the relevant individuals.

Conflict of Interest, Fraud and Compliance

ZINC is experienced in managing and mitigating the risk of Conflict of Interests, including across our recruitment, supply chain and the procurement process. We have employed a number of former government staff and ensure that they follow statutory regulations with respect to their responsibility to notify government pre-recruitment, mandating that their ZINC employment contract is conditional on them doing so and that they shall not engage in any policy shaping or business positioning on ZINC's behalf whilst in government employment. We will act subject to government conditions on a prospective employee, including restricting lobbying activity, contractually holding them to any confidentiality clauses and restricting them from working directly on any commercial activity related to their previous role. Placing undue pressure on or using influence with former colleagues to benefit ZINC is neither condoned nor allowed.

ZINC has harmonised our own established internal fraud processes with DFID's 2011 Independent Commission for Aid Impact (ICAI) report to ensure we meet and go beyond government best practice. A dedicated member of the Advisory Panel also acts as our internal compliance lead to provide advice, training and awareness-raising to staff on internal fraud measures and reporting guidelines. Segregation of duties is imperative to prevent internal fraud.

Our Knowledge and Experience in Developing Effective Risk Plans

We approach risk planning in a way that responds to: (1) the evolving tactics used against partners and (2) the need to grade risks according to their severity and urgency and respond accordingly. Broad and continuously updated situational awareness of each region and the Kremlin's interests and tactics is at the core of our risk planning. A subset of operational risk and safeguarding risks may be to: **individuals (physical/ reputational/ emotional), property, digital systems, and legal.** Network Managers will combine the consortium's context-awareness with their knowledge of individual Network Members to populate Member-level risk registers, feeding into the project's overarching risk register (see 1.11 for more detail).

Effective risk planning requires a realistic understanding of what materialisation would mean in practice for staff, Network Members and other partners, whether operational collapse or physical or emotional harm. By populating Network Member risk registers we help stakeholders better: **understand the risks** they take, helping them to put **basic deterrence measures** in place, for example, basic cyber 'hygiene' can act as a strong deterrent to interception as not a 'soft' target'; **equipping them with mitigation strategies** for when risks do materialize, including access to expert support, and finally in **building their long term resilience to risk,** for example through networking with like-minded organisations or ensuring they have organisational processes in place or basic insurance. Risk registers at the Network Member, regional and project level will highlight serious safeguarding risks on an ongoing basis. Review of these specific risks as part of weekly, monthly and quarterly project reporting will allow them to be escalated on a priority basis, where necessary, to allow for urgent intervention by the Consortium's risk and security partner, Toro (see 1.3 for more detail).

CASE STUDY: Safeguarding policies established for YouTuber network in Russia The Consortium established a robust safeguarding policy whilst establishing a network of YouTubers in Russia and Central Asia, who were creating content promoting media integrity and democratic values. This policy took measures to safeguard against Kremlin attack through actions including: supporting participants make and receive international payments without being registered as external sources of funding; managing their online profiles to reduce their exposure to cyber-attacks, trolling and abuse; connecting Youtubers with local pro-bono legal support; supporting them to develop editorial strategies to deliver key messages, whilst minimising risk of prosecution under ill-defined censorship laws, and carefully managing project communications to keep their involvement confidential.

1.3 Safeguarding

ZINC holds a strict duty of care to its employees and has robust processes in place to meet, and go beyond safeguarding requirements for subcontractors and partners, such as Network Members. Our consortium comprises experts in safeguarding and risk management, including Toro Risk Solutions, Jessikka Aro, a Finnish journalist and advisor on withstanding personal attacks as a result of exposing disinformation, and James Wilson, a specialist in legal compliance as a component of safeguarding and dealing with the threat of litigation.

These advisors, together with our Management and Security teams will oversee the safeguarding of project stakeholders on the ground including, but not limited to: project staff, freelancers, Network Members and training partners. We manage safeguarding responsibilities by (1) planning - ensuring we have the correct project policies and procedures, identifying risks and making incident response plans, (2) monitoring – exchanging information on context and on-the-ground developments through the project management structure, and (3) responding – putting incident response plans into action on the ground in order to limit harm in urgent safeguarding situations.

Planning

Toro will work with Network Managers to conduct a **physical and cyber security review** and make recommendations to address them, as well as populating **Risk Registers** with serious potential safeguarding risks highlighted (see 1.11 for more detail).

At the project level, **safeguarding protocols** will be developed within one month of inception covering individual, property, IT and Cyber, and legal risks. These protocols will help Network Managers identify safeguarding situations, triage them, take immediate mitigation steps and escalate to the Project Director (or other member of senior management) where appropriate[5]. Safeguarding our partners, stakeholders and staff across both online and offline activities is paramount to the work that ZINC carries out across all our projects. In light of the recent sexual exploitation and abuse in the aid sector, we have bolstered our focus on ensuring that across our organisation there is the moral leadership to provide guidance on what is and isn't acceptable behaviour on projects. We are amalgamating DFID's new Code of Conduct with our own policies, as well as including information and contact details for the FCO's Anti-Fraud and Corruption Unit (AFCU), and already have in place the systems, culture and transparency required to protect vulnerable individuals. We have managed to create a culture of respect and integrity by promoting ZINC's values at the recruitment stage, staff induction and employee annual performance reviews.

All staff are required to undertake various training modules using our online CascadeGo HR system, including Safeguarding, Data and GDPR Regulations, and Code of Conduct and Ethics. Our Safeguarding training module includes awareness of modern-day slavery and human rights abuses. Additionally, we will provide staff updates and hold regular refresher ethical training for staff and partners. Our policies will flow down to partners and stakeholders who are required, by our due diligence procedures, to take reasonable steps to ensure that in carrying out activities, they and their employees and directors comply with all applicable laws.

ZINC has a workforce whistleblowing policy in place for staff to anonymously raise concerns, administered by ZINC's Head of HR, and which is available to all staff and subcontractors. This service is fully supported at the Board level and Project Management level. The helpline details and information are contained within ZINC's Employment Handbook.

For key specific safeguarding risk categories, **Incident Response Plans** will be designed by Toro and the Advisory Panel to regulate how the Project Director – with appropriate support – will mobilise the project's resources to respond to serious and urgent safeguarding situations that have been escalated by Network Managers. This will ensure the right steps – whether deployment of a crisis communications team, additional security to a site, emotional support or demobilisation of staff – are taken as quickly as possible when the need arises.

Safeguarding will also be ensured by providing the most high-risk organisations with an additional layer of support. For the 10 Members deemed to be highest risk, this will include a comprehensive site visit to assess

[5] Whilst best practice safeguarding protocols exist for journalism, we are not aware of any tailored to counter-disinformation work. As part of our *Scale* strand, we aim to establish these safeguarding protocols and promote adoption across the wider sector.

their physical and cyber security requirements. Drawing on Toro's expertise, these assessments will be used to build a risk management framework to cover risks to Network Members and the project.

We will also safeguard by:

- **Reducing libel risk** through training on how to avoid engaging in practices that could provoke libel complaints, and reviewing key pieces of content
- **Setting up adequate insurance and support provision** with dedicated budget for professional indemnity insurance, which organisations themselves will take out, and we will also encourage organisations to find legal pro-support locally and broker connections when necessary
- **Providing basic legal training** in GDPR, how to protect themselves against corruption risks and other elements in order to ensure they are operating within all applicable legal frameworks and ethical guidelines
- **Upskilling in crisis communications** in the event of an attack, organisations will need to rapidly respond with precision and in a way that limits their reputational risk. We will train them in skills including crisis communications, safeguarding team members, designing emergency protocols, and will provide a rapid response support service
- **Cyber security** training and support will be delivered, including a secure communications portal for project communications, reducing the risk of attack

Each member will be trained and supported to develop and maintain a risk register, covering the risk categories outlined above. These will feed into the project-level risk register, owned by the Project Director, which will be reviewed and reported on weekly, and comprehensively reviewed with the support of an independent risk and security advisor monthly, prior to contract management meetings.

Monitoring

Real-time monitoring of safeguarding issues is undertaken by Network Managers. Information on overall context and threat levels is communicated from the Network Hub to each regional cluster. On a monthly basis, Network Managers use this information and their knowledge of Network Members and other partners' activities to set their monitoring posture and reacquaint themselves with specific safeguarding protocols and response plans as necessary.

In this way the Project Board stay aware of the general level of risk at all levels, and maintains an appropriate risk monitoring posture, ensuring that safeguarding incidents are properly triaged and escalated at speed if they do arise.

Responding

Serious and urgent safeguarding issues are escalated to senior ZINC management (we operate a 24/7 'on-call' system). The responder will cascade the notification to other senior management and the project's risk advisor, Toro, who will put the relevant Incident Response Plan into action, mobilising project resources as required. Across the life of the project, we have budgeted for incident response provision, at 278 days of legal support (including support for individuals harassed by the police or administrative authorities) and 300 days cyber and physical security support.

1.4 Curriculum Vitae

List of Project Staff to deliver against the Terms of Reference:

Project Board

- Louis Brooke (ZINC Network)
- Amil Khan (Aktis)
- Chris Donnelly (The Institute for Statecraft)

Core Project Delivery Team

- Urve Eslas – Project Director
- Mary Mitchell – Head of Network
- Roman Shutov – Network Manager
- Frank Williams – Network Manager
- Dalia Bankauskaite – Network Manager
- David Patrikarakos – Network Manager
- Ben Robinson – Network Manager
- Aric Toler – Open Source Researcher and Trainer
- Christiaan Triebert – Digital Forensics Specialist
- Tanya Bogdanova – Digital Strategist
- Jeremy Lloyd – Cyber Security Lead
- Chris White – Physical Security Lead
- Dan Williamson – Risk Management Lead
- James Wilson – Legal Advice
- Deepti Sastry – Monitoring and Evaluation Lead
- Alex Mackintosh – Creative Support
- Ziad Ramley – Digital Support
- Paul Birmingham – Project Manager
- Lyubomir Hristov – Line IT Support Analyst
- Russell Peacock – Grants Manager (Bio)
- Charlotte Beckett – Research Support (Bio)

Advisory Panel (Short Bios)

- Neville Bolt
- Peter Pomeransev
- Milica Pesic
- Jessikka Aro
- Ben Nimmo
- Graham Brookie

Louis Brooke – Project Board

Louis Brooke is the Managing Director of ZINC Network with more than 10 years' experience working in complex strategic communications, such as countering violent extremism, countering disinformation and promoting good governance. Louis' career has spanned a number of key leadership roles and has managed projects across the world, including the Baltics, East Africa, the Balkans and the Middle East. Working in partnership with national and international governments, Louis has delivered counter-disinformation projects in the Baltics, Ukraine, Georgia and Russia that range from delivering alternative and counter narratives from ZINC's flagship Russian-language social media platform (ZAG), to creating and working with a network of influencers to enhance their capabilities in disputing disinformation narratives. Louis has previously delivered advisory work for the Prime Minister of an Eastern Partnership regarding national disinformation influence. Louis regularly lectures at Kings College, London, regarding disinformation and strategic communications, and is on the board of NATO's Centre of Excellence for Strategic Communications.

NATIONALITY

British

EDUCATION

2006 - 2009 BA 1st class (Hons), Philosophy, Politics and Economics, University of Oxford

COUNTRIES OF WORK EXPERIENCE

Belgium, Georgia, Iraq, Kenya, Latvia, Lebanon, Pakistan, Somalia, Tunisia, Ukraine, USA

LANGUAGES

English (native)

RELEVANT PROJECT EXPERIENCE

Worldwide – ZINC Network, 2015 - ongoing, Managing Director

- Responsible for all aspects of International work for ZINC Network, across country offices in Kenya, Somalia, Tunisia, Estonia, Australia and Iraq.
- Developed a portfolio of work globally worth £8m p/a.
- Oversees all aspects of portfolio including strategy, creative, implementation, budget, client management and business development.

Europe – SCAT, 2014 - 2015, EU DG Home, Team Leader

- Established a team within EU DG Home to build the capacity of member states to undertake strategic communications campaigns around Counter Violent Extremism issues.
- Led a team of 6 established network of senior communications and counter terrorism officials from 24 member states within the EU which met on monthly basis of knowledge sharing and training sessions,
- Led 10 consultancy visits to different EU member states which involved on the ground research with senior politicians and officials from the police Ministry of Interior and intelligence as well as representatives from communities and media.

East Africa – ZINC Network, 2013 - 2015, US Department of State/UN, Head of East Africa

- Responsible for all of ZINC Network's operations across the region.
- Responsible for Somalia and Kenyan stakeholder engagement across the public/private sector
- Developed communications strategies for clients and acted as executive producer for TV and radio content.

UK – LRS, 2009 - 2013, Communications and Marketing Director

- Responsible for developing and implementing the marketing, communications and investment strategies for an innovative social enterprise providing a diverse range of financial services to excluded communities.
- Successfully developed and delivered an integrated marketing and communications plan achieving greater brand awareness, consistent messaging and increased turnover across various service areas.
- Led on raising investment for the company and successfully secured £4 million in grants and negotiated a further £22m in private funding.

Amil Khan – Project Board

Political and communications advisor. Experienced at providing strategic advice to political movements and established leadership at senior levels. Chatham House fellow. Former award-winning documentary maker and Reuters Middle East correspondent. Regular contributor to UK and international news media.

EDUCATION

BA Hons (2:1) Arabic and Farsi, Durham University, UK

LANGUAGES

Native English speaker, fluent in Arabic, fluent in Urdu, basic Farsi

PROFESSIONAL EXPERIENCE

Behavioural Communications Expert, Aktis Strategy, July 2017- Present

- Works across Aktis' portfolio of behavioural and strategic communications projects in Eastern Europe, North and East Africa and the Middle East
- Leads strategy research, design and implementation of the efforts to identify, map and mitigate the risks of nefarious narratives disseminated by domestic actors and adversary states to strengthen state stabilization and audience resilience
- Provides technical advice to setting up resonant narratives aimed at intergroup/interethnic dialogue and social cohesion via independent media support, StratCom campaigns and engagement with local influencers

Expert Advisor, UK Government, July 2017 – Present

- Prime Minister's Office: Senior advisor on Oman engagement. Relationship building, political analysis and liaison with multiple Omani government departments to develop the UK's engagement strategy
- Cabinet Office: Strategy advisor on government of Pakistan reform efforts. Leading on engagement with Pakistani government bodies to assess political will and capacity to develop institutionalization in state structures
- Ministry of Defence: Advice and support to UK military on efforts to develop politically-informed campaigning approaches

Associate Fellow of Chatham House, The Royal Institute of International Affairs, January 2018 – Present

- Policy research related to security, economics and diplomatic relations between Gulf and South Asian states

Project Director; Syria Armed Opposition Support; UK Ministry of Defence

- Led teams spread across Turkey, Jordan and Syria focused on building political coherence amongst the disparate groups that form the Free Syrian Army by engaging leadership figures directly, supporting them during negotiations and instilling concepts such as good governance and international humanitarian law.
- Served as key point of access and convener between FSA, regime figures and multiple security agencies during Track 2 negotiations aimed at reducing civilian casualties through aerial bombardment.

Political communications consultant, May 2014 – May 2015

- UK Military (Permanent Joint Headquarters): Lead embedded advisor to elite Kurdish Peshmerga units based in Erbil. Trained frontline officers in practical application of international humanitarian law. Established political structures to allow military forces to engage local populations and international bodies in line with international best practice.
- Amnesty International: Devised and delivered training sessions for Syrian civil activists in strategic communications, strategic planning and advocacy
- Private sector companies: Assessing exposure and risk to hostile action from extremists via physical or online targeting of facilities or employees in hostile environments

Advisor to the Syrian Opposition Coalition, UK Foreign and Commonwealth Office (FCO), February 2013 - May 2014

- Generated the political will amongst the coalition's leadership to institutionalise the body's structures, improve its ability to engage key audiences

- Led a team of Syrian specialists in generating and presenting strategic policy advice to senior decision makers, including senior political and military leadership figures
- Provided embedded strategic advice during key junctures of the conflict, including the intervention of Hezbollah into the conflict, the regime's use of chemical weapons and international peace talks

Project Manager – Pakistan Counter Violent Extremism, April 2011 – December 2012

- Engaged in extensive political contact with key Pakistani actors including officials, political figures, media owners and religious figures to inform the project's strategy and implementation plan

Strategic Communications Lead, Pakistan: Oxfam GB, November 2010 – April 2011

- Drafted in to help Oxfam GB manage its response to the 2010 Pakistan floods
- Led a team of media, advocacy and policy advisors engaging Pakistani decision makers to affect strategic change in policy

Subject Specialist – Counter Violent Extremism, September 2009 – November 2010

- Authored a review of Pakistan's extremism risk factors
- Engaged tribal leaders in Mali to assess resilience to Al Qaeda penetration

Produced and presented documentaries for Channel 4 and BBC 1, November 2007 to August 2009

- Channel 4 Dispatches: Jail to Jihad – Investigated criminal networks in the UK to map the growth of extremist ideology amongst violent criminals
- Channel 4 Dispatches: Jon Snow's Hidden Iraq – Investigated the scale of under-reported violence in Iraq during the height of the US surge by embedding with US and UK forces and interviewing Iraqi officials and insurgent leaders
- BBC Panorama: Hate on the Doorstep – Produced and presented a complex investigation into the abuse suffered by recent immigrants in deprived parts of the UK
- BBC Panorama: China's Secret War – Embedded with rebels in Sudan's Darfur region to uncover evidence of war crimes committed with Chinese assistance

PUBLICATIONS

- Khan, Amil 2013. "Pakistan and the Narratives of Extremism" United States Institute for Peace (USIP): Special Report
- Khan, Amil 2018. "Review: Taliban Narratives" International Affairs, Oxford University Press
- Frequent contributor to international publications and television news, including; Buzzfeed, Foreign Policy, Politico, Telegraph

OTHER SKILLS, TRAINING AND QUALIFICATIONS

- Security cleared
- Hostile environment trained

Christopher Donnelly – Project Board

Chris Donnelly is co-founder and co-director of the Institute of Statecraft, which works with international institutions, governments, academia and the corporate sector. The Institute maintains a large network of specialists and researchers on all aspects of international security, develops and runs educational programmes on international security issues, implements practical mechanisms to enable good governance, capacity-building and organisational reform in national and regional governments and major institutions, especially in the broader areas of national security.

EDUCATION

BA (Hons) Russian Studies, University of Manchester, 1969

LANGUAGES

Native English speaker, fluent in French, proficient in Russian, proficient in German

PROFESSIONAL EXPERIENCE

Co-Founder Co-Director, The Institute of Statecraft, 2010 – Present

Research interests include:

- Dynamics of change in the international security scene
- Impact of Globalisation and of the revolution in the nature of conflict and competition on national and international institutions
- Growing importance of non-military threats to international and national security and the development of appropriate responses
- Ambiguous warfare; disinformation and malign influence.
- Alternative models of governance for the management of national and international security.

The Senior Fellow, Defence Academy of the UK, 2007 – 2010

- Responsible to the Director General of the Defence Academy for developing concepts for the transformation of the Academy from a purely defence establishment to one dealing with wider national and international security issues.

Head of the Advanced Research and Assessment Group, Defence Academy of the UK, 2003 – 2007

Devised, set up and ran the Advanced Research and Assessment Group which:

- Generated and stimulated new thinking on current international security issues, and harnessed this to support policy-making
- Developed new analytical tools and learning mechanisms for the UK national security education system.
- Worked to refocus the UK strategic studies community and the academic community onto new national and international security issues.
- Developed and implemented a programme for capacity building and conflict resolution in the Middle East and Northern Iraq
- Developed and implemented programmes for leadership, strategic thinking and good governance for security institutions in transition in ME/NA countries.
- Developed a programme for engaging the Armed Forces in the integration of ethnic communities into the UK social mainstream and in supporting counter-radicalisation.

Special Adviser for Central and Eastern European Affairs to the Secretary General of NATO, 1989 – 2003

Served four Secretaries General: George Robertson, Javier Solana, Willy Claes and Manfred Woerner

- Prepared and delivered policy briefs and advice to the Secretary General, NATO Council, and leaderships of NATO members and partner countries;
- Created a forum for East-West dialogue after the collapse of the USSR, bringing together highly placed policy makers, opinion formers and decision takers and establishing and validating mechanisms for cross-cultural communication and collaboration on international security issues;
- Developed collaboration with EU counterparts to support the evolution within the EU of competencies in international security issues;

- Devised and implemented programmes to improve policy-making and decision-taking in Central and Eastern European countries, contributing to creating the political, economic and military transformation necessary for NATO and EU membership;
- Introduced into NATO the study of new security issues and outreach to countries of the Middle East and Far East. This provided a stimulus to accelerate the development of NATO from an almost purely military and defence alliance to one addressing wider aspects of international security.
- Set up an innovative internship programme, recruiting and training over 100 postgraduates to analyse current international security issues and to understand how to operate in a difficult multi-national environment.

Director, Soviet Studies Research Centre, The Royal Military Academy Sandhurst, 1979 – 1989
Developed the Centre from a tactical-level research and education body serving the Army to an organisation addressing political and strategic issues, advising the highest levels of government in the UK, US and several European countries.

- Educated a generation of British army officers to understand the military and political thinking of other countries and cultures
- Developed, based on a true understanding of different cultures and mentalities, a historically innovative methodology of objectively studying other countries and armed forces from their point of view: how they saw themselves and their relationship with the West
- Ran a programme with China (1982-7) to assist in reviving their international security studies capability in governmental and academic institutions
- Improved the process of 'red teaming', providing a reliable and responsive opponent to test military training and development. Author of the official UK Army training manual on understanding Soviet/Russian military thinking.
- Provided the UK contribution to the US programme of reverse engineering and analysis of foreign weapons and equipment.

PUBLICATIONS

- Heirs of Clausewitz – Institute for European Defence and Strategic Studies 1984
- War and the Soviet Union – Janes Educational Video series 1986
- Red Banner: The Soviet Military System in Peace and in War - Jane's 1988
- Gorbachev's Revolution: Economic Pressures and Defence Realities (Ed) - Jane's 1989 - 2004
- Nations, Alliances and Security – Institute for Transitional Democracy and International Security - Hungarian Academy of Sciences, Budapest 2004
- Editor, The British Army Official Yearbook– Ministry of Defence 2009-current
- Over 100 articles in professional defence and academic journals

Urve Eslas – Project Director

Urve Eslas is a strategic communication and foreign policy expert with more than 13 years' experience and with a keen interest in the Baltic States, Eastern Europe and Russia. Urve has worked for Estonia's largest daily newspaper, Postimees, as well as the Estonian Public Broadcaster, Center for European Policy Analysis and the Office of the former President of Estonia, Toomas Hendrik Ilves. Urve worked for a StratCom program of a Washington-based think tank, the Centre for European Policy Analysis. She has been developing and maintaining the network of government organizations, NGOs and media organizations in Baltic States, giving platforms for NGO's working on disinformation in Estonian media, organizing gatherings, discussion groups and media campaigns to increase media integrity and information resilience. She has been actively involved in numerous conferences, forums and discussion groups, and has briefed governments and NGOs on information warfare and strategic communication in Europe and the United States, including the US National Intelligence Council, the US State Department, the US National Security Council, and NATO.

NATIONALITY

Estonian

EDUCATION

2004	MA Philosophy, Estonian Institute of Humanities
2003	BA Humanities, Estonian Institute of Humanities

COUNTRIES OF WORK EXPERIENCE

Estonia

LANGUAGES

Estonian (native), Russian, English

RELEVANT PROJECT EXPERIENCE

Estonia – 2016 – ongoing, Office of the President of Estonia, Advisor to the former President of Estonia Toomas Hendrik Ilves

The Office of the President supports the President and former Presidents in fulfilling their official duties. The Office manages the domestic and foreign communications of the President and former Presidents, information exchanges with media, the public and other stakeholders. Urve is responsible for strategic planning, public engagement, political affairs, and communications.

Estonia – 2016 – ongoing, Centre for European Policy Analysis, StratCom Initiative, Adjunct fellow

The Centre for European Policy Analysis is a research institute based in Washington, DC, dedicated to the study of Central-East Europe and Russia. Urve is responsible for monitoring and analysing disinformation in Estonia and the neighbouring countries, developing and maintaining the NGO's network in Baltic States, briefing governments and NGOs on information warfare and strategic communication in Europe and the United States.

Estonia – 2007 – 2016, Postimees daily newspaper, Opinion page editor

Postimees is Estonian biggest daily newspaper. As an opinion page editor Urve was responsible for strategic planning of opinion pages, developing and maintaining contacts with government organizations, NGOs, media organizations and opinion leaders, organizing conferences, gatherings, discussion groups, writing editorials and columns. In her editorials she was concentrating on politics, information- and cyber warfare, media integrity and information resilience. In 2007, after Russia's active disinformation campaign in Estonia, Urve established an information resilience section that translated and published regularly opinion pieces by Western journalists and analysts, and that later gave a platform for Estonian voluntary organization Propastop that monitors, analyses and explains disinformation attacks in Estonian and Russian media.

Estonia – 2013–2016, Estonian Public Broadcasting, Radio commentator

Estonian Public Broadcasting is a publicly funded radio and television organization in Estonia. The role of radio commentator is to analyse current events and developments both in domestic and foreign politics. In her comments Urve was concentrating on Russia, on information warfare and on strengthening the civil society.

Estonia – 2012 – 2016, Radio Kuku, Host of the weekly radio program "Vahetund Postimehega" ("Recess with Postimees")

Radio Kuku is politically independent privately-owned radio station in Estonia. “Vahetund Postimehega” (“Recess with Postimees”) is a weekly radio program concentrating on current affairs. As the program host, Urve’s role was strategic planning of the program, creating and maintaining the network of opinion leaders, and leading the discussions.

Estonia – 2014 – 2016, Estonian Public Broadcasting, Host of the weekly radio program “Vasar” (“Hammer”)
Estonian Public Broadcasting is a publicly funded radio and television organization in Estonia. “Vasar” (“Hammer”) is a weekly radio program on culture and politics. As a host, Urve’s role was strategic planning of the program, creating the network of opinion leaders, and leading the discussions.

Mary Mitchell – Head of Network

Mary has a decade of experience in communications spanning a variety of sectors, including international development, media development and refugee assistance. She currently oversees delivery of projects ranging in value from $500,000 to $1,000,000 for clients including the State Department and the British Foreign and Commonwealth Office, specialising in media development and strategic communications. Mary is a PhD Candidate in Media Arts, has an MSc in Forced Migration from Oxford University, and has been published in outlets including the New Statesman and the Guardian as well as authoring a variety of academic journal articles and book chapters.

Mary's role at ZINC focuses on Central Asia and Eastern Europe, she has spent a total of 18 months in Kyrgyzstan and Kazakhstan over the course of her career. She's designed and delivered communications training for NGOs including Oxfam, Mercy Corps and Save the Children in contexts as diverse as Bangladesh and Lebanon, and run strategic communications projects for the State Department in South Asia and Ukraine.

NATIONALITY

U.K.

EDUCATION

2013-2018	PhD Candidate, Media Arts, Royal Holloway University of London, London (submitted)
2007-2008	MSc, Forced Migration, University of Oxford, Oxford
2004-2007	BA (Hons), History, University of Manchester, Manchester

COUNTRIES OF WORK EXPERIENCE

UK, Kyrgyzstan, Somalia, Tunisia, Latvia, Lithuania, Estonia, Bangladesh, Pakistan, India, Lithuania, Latvia, Estonia, Ukraine, Russia

LANGUAGES

English (native), Russian (intermediate), Arabic (basic)

RELEVANT PROJECT EXPERIENCE

Russia, Latvia – Audience Segmentation and Analysis for Russian-language independent media outlets, May 2018 – Present, NED, Senior Account Director

Overall responsibility for delivery for project including:

- Managing research and digital teams
- Responsibility for multi-stakeholder relationships with media outlets, client, and research partner
- Liaising with research partner (King's College London), linking outputs from data scientists to in-house audience segmentation and targeting expertise
- Developing project workplan and outputs
- Developing training and mentoring programme for participating outlets
- Overseeing monitoring and evaluation

Latvia, Lithuania, Estonia – Baltic Independent Media, April 2017 – April 2018, FCO, Head of Capacity Building/ Senior Account Director

Worked on the project in two roles, overseeing training and mentoring deliverables

- Design of Media Accelerator programme, including recruitment, work plan, learning plans
- Research into media environment in the Baltics
- Delivery of training programmes
- Overseeing a mentoring programme
- Multi-stakeholder management across four countries
- Overseeing monitoring and evaluation

Bangladesh, Pakistan, India – Building Credible Voices, Jan 2017 – Present, U.S. State Department, Head of Capacity Building

- Overseeing the launch of a two-year project in South Asia, including recruitment of local staff and project management
- Design and delivery of bespoke training sessions
- Design and delivery of training sessions focusing on filmmaking, social media and campaign planning. Adapted for various international contexts including Somalia and South Asia
- Establishing agency-wide processes for capacity building

Tunisia – Jasoor Participatory Media Project, 20017, U.S State Department, Head of Capacity Building
A participatory photography project implemented throughout Tunisia in partnership with youth organizations and schools, designed to increase trust between youth workers and young people.

Somalia – Suuqa, 20016, U.S. State Department, Head of Capacity Building
Training civil society organizations in Somalia to run online and offline campaigns challenging messaging from violent extremists, promoting peace, integration, stability and development.

OTHER PROFESSIONAL EXPERIENCE
London – November 2015 – December 2016, Account Director
Overseeing communications activity across a network of civil society organisations working on community cohesion in the UK.

- Developing key messages for campaigns and mapping delivery across platforms
- Communicating regularly with clients on status, timeline, deliverables and reporting
- Project Management; leading production and creative teams to deliver client work at agreed timescales
- Developing content proposals in response to news and current affairs
- Analysing client campaign results and data, and regular reporting and presenting of campaign/account performance across multiple channels
- Designing and delivering training sessions on communications planning (UK and International)
- Recruiting and line managing junior members of the team
- Overseeing relationship management with eight account leads and 40 civil society organisations
- Advising on programme development for projects in South Asia and Eastern Europe

London – August 2015 – November 2015, Content Strategist
Planned, delivered, monitored and evaluated CVE campaigns for governmental agencies and civil society organisations based on understanding clients' needs, and audience research.

- Created comprehensive digital profiles for clients based on analyses of their target audiences
- Provided expertise to clients through delivering regular training sessions and creating resource guides
- Conducted audience research using tools including Brandwatch.
- Developed an agency-wide process for content optimisation

London – July 2013 – July 2015, White Fuse Media, Content Strategist
Managed web content strategy for a diverse portfolio of organisations in the third sector including multi-language projects with complex content requirements.

- Drove search engine optimisation programmes to increase organic ranking
- Developed digital marketing strategies for fundraising and awareness raising campaigns
- Conducted user research and designed user journeys
- Planned, managed and delivered targeted email marketing campaigns

London – January 2012 – July 2013, Refugee Support Network, Communications Manager
Directed communications and campaigns development for one of the UK's leading refugee charities.

- Championed communications within the organisation, building a communications and fundraising team
- Developed KPIs and reporting methodologies
- Wrote best practice guide for media engagement with refugee children

London & Kyrgyzstan – July 2011– June 2012, Freelance, Journalist and Filmmaker
Researcher credits including BBC documentary on institutionalisation of children in Ukraine

- Shot and edited films for charities including UNICEF, Tearfund and RSN
- Writing published by outlets including The New Statesman, AJE, and the Guardian

London – August 2010 - July 2011, Equip, Refugee Project Coordinator
Managed a network of faith-based projects supporting refugees around the UK in key dispersal areas

Kyrgyzstan – February 2009 – September 2009, Acted, Reporting Intern
Reported to donors including World Food Programme, European Commission, and USAID on development and disaster relief projects in Kyrgyzstan

Roman Shutov – Network Manager

Roman has more than 10 years' professional experience in strategic communication, including research and analysis of Kremlin propaganda in the EaP for the Baltic Centre for Media Excellence; monitoring freedom of speech, quality of media, journalist ethics, manipulations and propaganda in media on behalf of Detector Media; and network development / media needs assessments. Roman's PhD was conducted at the Academy of Science of Ukraine, with his thesis exploring 'Foreign information influences as Factor of State Information Policy in Ukraine'.

NATIONALITY
Ukrainian

EDUCATION

2007 – 2013	PhD in Political Science, Koretskyi Institute of State and Law, Academy of Science of Ukraine
2002 – 2007	Master Degree in Political Science, East Ukrainian Naitnoal Dahl University

COUNTRIES OF WORK EXPERIENCE

UKRAINE, LATVIA

LANGUAGES

Ukrainian (native), English, Russian, German, Polish

RELEVANT PROJECT EXPERIENCE

Ukraine – 2018 to present – Baltic Centre for Media Excellence – Strategic Advisor
Responsible for research and coordination of donors and partners in the EaP countries in terms of media development and media literacy; research and analysis of Kremlin propaganda in the EaP; and consulting donors, governments, NGOs, media in media development and information security.

Ukraine – 2014 to 2018 – Detector Media – Program Director
Supervising the program performance related to freedom of speech, quality of media, journalism and ethics, manipulations and propaganda in media. Specific activities included preparing methodologies for media monitoring, co-ordinating monitoring teams, preparation and publication of analytics reports of Ukrainian and foreign audiences; consulting government in information security; and drafting legislation.

Ukraine – 2012 to 2014 – MAMA86 – Development Advisor
Responsible for PR and communications, consultation in operation and strategic planning and network development.

Ukraine – 2008 to 2012 – CCC Creative Centre – Media Project Manager
Management of separate local media-related and local democratic development projects funded by EU, UNDEF and USAID, including analysing local media and media needs assessments.

Frank Williams – Network Manager

Frank Williams has extensive experience in developing media outlets’ and NGOs’ skills across Europe, Central Asia and Russia. Frank is the Chair for the Prague Centre for Media Skills, delivering a substantial number of workshops for reporters and journalists. Frank was responsible for maintaining and developing a network of affiliate broadcasters to carry RFE/RL programmes locally in the Russian Federation, Ukraine, Moldova, Kyrgyzstan and Kazakhstan; and was Project Manager for BBC World Service Training.

NATIONALITY
British

EDUCATION

M.Phil., St Andrews University
B.Sc. Hons, Russian Language and Soviet Studies, University of Surrey

COUNTRIES OF WORK EXPERIENCE

Czech Republic, Georgia, Hungary, Russia, Moldova, Kyrgyzstan and Kazakhstan

LANGUAGES

English (native), Russian, Czech, French, German

RELEVANT PROJECT EXPERIENCE

Czechoslovakia – 2012 to present – Chair
Provide training support to independent, democratic media outlets and journalists in the countries of the former Soviet Union. Initiating and organising training workshops in Prague for reporters and editors from Georgia, Abkhazia, South Ossetia and the North Caucasus region.

2001 to 2010 – Radio Free Europe / Radio Liberty – Director
Responsible for reviewing broadcast and web product of all 28 of RFE/RL's language services and units; producing a formal review document analysing content and presentation quality; leading a discussion of findings at annual review meetings for each language; making recommendations for content development and staff training to strengthen output. Responsible for maintaining and developing network of affiliate broadcasters to carry RFE/RL programmes locally in the Russian Federation, Ukraine, Moldova, Kyrgyzstan and Kazakhstan. Responsible for organising an annual conference of affiliate broadcasters from across RFE/RL's target region, held alternate years in Prague and one of the countries of the broadcast region

1995 – 2001 – BBC World Service Training – Project Manager
Project Manager for BBC Schools of Broadcast Journalism in Ekaterinburg, Russian Federation, and Bucharest, Romania, funded by the UK government's DFID and the Soros Open Society Foundation. Project Manager, training programme for Georgian Public Television and Radio, funded by EU Tacis.

Dalia Bankauskaite – Network Manager

Dalia has more than 15 years' overall professional experience in strategic communication, advising on euro-integration, state programs and state reforms, free trade agreements, investment promotion and image building state institutions and private sectors. A key component of her career has been in transatlantic politics; developing and implementing a comprehensive strategy to counter Russian disinformation in the CEE region. She has over ten years' specific experience in EU-related integrated communication strategy development and implementation that started from drafting the EU promotion strategy and action plan (campaigns) for the EC Delegation in Vilnius, Lithuania, to be followed by Lithuania's accession to the EU (5 years of a senior management position in the Government on communication issues); communication strategy and visibility guidelines for Structural Funds in Lithuania; or providing assistance to the BiH Government in its European integration process and advisory support to the Ukrainian Government for Association Agreement and DFTA implementation in Kiev, Ukraine, and External communication strategy on AA/DCFTA for Georgia.

NATIONALITY
Lithuanian

Education

2002 – 2003	Executive Master of Business Administration, Baltic Management Institute
1994 – 1995	MSc in European Studies, London School of Economics
1992 – 1993	Diploma in International Relations, London School of Economics and Political Science (LSE)
1981 – 1987	Diploma in English, Vilnius University

COUNTRIES OF WORK EXPERIENCE
Ukraine, Georgia, Bosnia and Herzegovina, Latvia, Estonia, Nordic countries AND Russia
Languages
Lithuanian (native), Russian (native), English

relevant project experience
Lithuania – Strategic Communication Program Development - 2016 to present – Center for European Policy Analysis - Fellow in Residence, Communication Consultant
Responsible for bringing together leading journalists, activists and media and policy analysts from Europe's frontline states and utilizes their expertise to develop an analytical toolkit for effectively dealing with Russian disinformation at the institutional, strategic and conceptual levels.

Georgia – 2016 – Ministry of Economy and Sustainable Development – International Communication Expert
Responsible for reviewing existing communications on DCFTA in Georgia to align messaging; mapping of institutions involved in investment promotion including objectives and priorities; analysis of investment opportunities under the DCFTA and identification of target markets and sectors; development of messaging aimed at attracting investors to Georgia under the DCFTA; agreement of strategy and approach with key stakeholders; development of action plan for implementation, including a monitoring and evaluation mechanism.

Lithuania – 2013 to 2016 – The Seimas of the Republic of Lithania – Advisor of EU Relations
Advisor to the Committee on European Affairs and later Advisor to the EU Information Office: parliamentary control of national executive institutions (ministries) in the ECOFIN (Economic and Financial Affairs Council) field; EU economic governance, financial sector issues; parliamentary monitoring of Eastern Partnership program; communicating parliamentary initiative among EU members states parliaments for broader support (political and economic) of Ukraine as well as other Eastern partnership members (Moldova, Georgia). Provided advise on strategic communication of the Government on introducing euro in Lithuanian in January 2015. Dalia contributed to the Parliament's communication with the public at large and its target groups, launching public (parliamentary) diplomacy initiatives, closer cooperation with NGOs, social partners, business sector in European integration issues; monitoring the EU and other international assistance management in Lithuania, assessing its integrated communication; development of parliament's communication in social media. Dalia's responsibilities included sharing Lithuanian experience on strategic communication for European integration with EaP countries politicians and civil servants (presentations, meetings, video conferences); implementing events

in the parliamentary dimension of the Lithuania's Presidency to the EU Council (such as COSAC, Conference of Speakers EU parliaments).

Ukraine – 2014 to 2015 – Secretariat of Cabinet of Ministers, Office of EU Integration – Communications Strategy Expert on DCFTA

EU advisory support to the Government Office for European Integration and building up an effective coordination mechanism for the EU – UA AA implementation. Consultancy and experience sharing on AA and DCFTA strategic communication with the Government institutions; methodological proposals on drafting a Communication strategy for the EU-Ukraine association Agreement implementation (including DCFTA).

Lithuania – 2012 to 2013 – PTIAHCR – Senior Expert on Integrated Communication
Senior Expert on Communication Management of the "Promotion of Tourism by Increasing Awareness of the History and Culture of the Regions" international project which was financed by the European Neighbourhood and Partnership Instrument 2007-2013 Cross Border Cooperation Programme Latvia - Lithuania-Belarus. Responsible for the "MobileTour in Druskininkai (LT) and Grodno (BY)" activity of the project. She provided advise in the field of strategic communication, in particular to design of the communication campaign and development of marketing solutions based on 2D technologies (multifunctional mobile information dissemination system (Mobile Guide) and code scanning solutions)) and integration into the marketing of the region, which also included selection of historical, cultural heritage and nature objects attractive to tourists, their description (copyrighting) in four languages; production of photos; adaption for mobile phones, map design, four tourist route design, coding by UpCode/QR; training local government marketing staff and hospitality sector representatives (hotels, restaurants, entertainment sector, ect.) of mobile application and on further development of mobile tours. A project manager for the "Open code –CITIZEN" project aiming to increase student motivation and opportunities to initiate their own active participation in civic activities; design and implementation of a communication campaign through full media communication, including social media, workshops, seminars and conferences and social advertising. The visibility materials developed as part of this campaign have been awarded a prize for creativity.

Lithuania – 2011 – Ministry of Foreign Affairs – Communications Strategy Expert
Responsible for delivering a feasibility study on "Solutions for the communication strategy and action plan for Lithuania's Presidency at the EU Council"; managed drafting of the feasibility study and recommendation for communication strategy during Lithuania's Presidency at the EU Council.

David Patrikarakos – Network Manager

David is an international author, journalist, analyst and producer with an extensive track record in high-end international affairs and the study of disinformation. As a foreign correspondent, he has reported from across the world for a variety of leading US, UK and international publications. He covered the Greek crisis and spent over a year on-the-ground covering first the war in Ukraine where he developed an understanding of information war. As well as his journalistic writing, he has worked with think tanks and the British government to help create policy and lectured at institutions across the UK and USA. He is a contributing Editor at the Daily Beast, a Contributing Writer at Politico Europe, a Poynter Fellow in Journalism at Yale and an Associate Fellow of the Institute of Iranian Studies at the University of St Andrews. He has written for The New York Times, Financial Times, Wall Street Journal, The Sunday Times, Newsweek, Guardian, Time, Telegraph, Spectator, London Review of Books, Independent, Prospect, BBC, Politico, Foreign Policy, New Statesman, Times Literary Supplement, New Republic, CapX, Literary Review, CNN, Mashable, Tablet, National Interest, Reuters and many others.

NATIONALITY
British

EDUCATION

2004-2008	MLitt Oriental Studies and Middle Eastern Studies, University of Oxford, UK
2000-2001	Graduate Diploma in Law, Nottingham Law School, UK
1996-2000	BA English Literature and Language, University of Reading, UK

COUNTRIES OF WORK EXPERIENCE

DR Congo, Egypt, Greece, Iran, Israel, Qatar, UK

LANGUAGES
English (native), Greek, Farsi

RELEVANT PROJECT EXPERIENCE

2009–2011 & 2014–present, International Crisis Group, Consultant
David co-authored a report on the Ukraine crisis and co-authored another report on Iran's nuclear programme read by senior policymakers in the US and Europe.

2013–2014, Blakeway Productions, Development Producer
David developed ideas for a variety of broadcasters including BBC, ITV and Channel 4.

2010–2013, various companies, Assistant Producer
David worked for Ultramarine Films, Watershed Films, and Blakeway Productions on developing ideas for a variety of broadcasters including BBC, ITV and Channel 4, arranging shoots, and outlining films and their storylines.

2010–2013, OR Media, various roles
David worked on films for the BBC, Channel 4, ABC, Al Jazeera, Discovery and Al Arabiya to develop ideas and produce content on topics including the Greek financial crisis, the UN Mission in DR Congo, and Iran's nuclear programme.

Ben Robinson – Network Manager

Ben Robinson is a Fellow of the Institute for Statecraft with responsibility for the Integrity Network in Ukraine, website content and imagery, understanding and countering visual disinformation and developing collaborative training materials to help cultivate critical thinking and discernment and build resistance to disinformation. He plays a regional role in facilitating the sharing of best practice between partners in Ukraine, Lithuania, Bosnia and Herzegovina, Armenia etc. Ben has 25+ years' experience of travel, research, networking and NGO development through eastern and central Europe, including serving as Director of the Centre for Leadership in Kyiv, Ukraine with responsibility for expansion of training centres in Kharkov and Yerevan, Armenia. He's also a photographer and visual story-teller for the Prince's Trust, UK Child-Aid, Revitalise etc, with exhibitions in London (House of Commons, Ukrainian Embassy), Oxford, Vienna and Kyiv (Ministry of Education). This work includes an extensive, photo-documentary focus on the impact of the war upon civilians in Donbas (eastern Ukraine) from 2014-present, including numerous visits along the contact line and first-hand experience of the impact of Russian aggression and disinformation. He's currently working with the Ministry of Health in Ukraine to help visually communicate needed reform priorities and counter Russian-lead disinformation strategies to undermine those efforts.

NATIONALITY

British/ USA

EDUCATION

2001	London Business School, Inter-personal Skills for Senior Managers
1992 – 1995	University of Oxford, BA (Hons.) PPE (Philosophy, Politics and Economics)

COUNTRIES OF WORK EXPERIENCE

UK, Ukraine

LANGUAGES

English, Russian (both fluent)

RELEVANT PROJECT EXPERIENCE

UK– Russian Disinformation, December 2016-present, Institute for Statecraft, Fellow

Focus on project to identify and counter Russian disinformation, particularly the use of manipulated and false imagery. Responsible to develop Statecraft "cluster" in Ukraine as part of a wider European network.

UK/Ukraine – February 2013 – present, findyourvoice.me.uk, Founder

[Visual story-telling and media support for clients including Prince's Trust, UK, IOM, RLC Foundation, Ardenia Group UK, and CILT Dubai, UAE. Extensive photography portfolio including political communication, NGOs, corporate work and private sector.

UK – April 2011 – February 2013, Event Business Academy, Programme Director

Responsibility for course design, sales strategy and partner recruitment for an educational start-up that delivered a highly acclaimed programme to over 80 students from 23 countries in its first year of operation. Diverse responsibilities included sales strategy and delivery, website launch, international partner recruitment (including Sochi 2014 Committee), accreditation oversight, training content design, delivery and photography support.

Ukraine – 2004-2010, Graduate School of Business and Management, Part-time lecturer/ consultant

Delivered and designed training for modules including Managing Creativity, Effective Communication, Leadership Principles, Creative Life Planning

Responsible for seminars including "Delivering Presentations", "Cross-cultural Business Communication" to USAID staff, September 2009. "Coaching and Mentoring Young Leaders", Merck Pharmaceuticals, Ukraine

Executive Management Team, July 2010.

Ukraine – 1997 - 2004, Centre for Leadership Development, Kiev Executive Manager
Financial planning, budgeting and reporting to international partners. Community networking with partners to facilitate wider consultation and trainings. Strategic planning and coordination with key stake-holders: faculty, staff and students. Design CLD curriculum and recruit instructors from organisations including the World Bank, UN Food and Agricultural Program, Proctor and Gamble, IBM, Kimberly-Clark, Kodak.

Aric Toler – Open Source Researcher and Trainer

Aric Toler has more than 10 years' experience as an open source researcher, intelligence specialist and working with journalists, and is currently the lead researcher and writer for Eastern Europe and Eurasia at Bellingcat, a project aimed at publishing research and analysis derived solely from open source intelligence, such as satellite imagery, social media, mass media reports, etc. He

Aric has supported journalists and media outlets to build capacity in digital journalism, having designed and delivered capacity building programs for over 160 Russian-speaking journalists, researchers, and activists in digital journalism, research and verification skills in Eastern Europe, Caucasus and Central Asia. He has co-led and supported journalists in digital forensics and verification workshops in English and Russian in numerous contexts and information environments, from Ukraine to Malaysia and presented best practices of digital journalism and strategies of integrating them in media on academic events e.g. Open Source Intelligence Dissemination Conference in Rome and "Verifying News" conference at MIT.

Aric has robust understanding of power dynamics between Russia and Eastern European states as the #MinskMonitor project lead, tracking the ongoing conflict in eastern Ukraine and the ramifications of the Kremlin disinformation efforts across the region, focusing on digital evidence and fact-checking. He has also developed an extensive network of journalists, academics and media professionals as the contributor of RuNet Echo and by participating in events, workshops and conferences in the region, such as MezhihiryaFest in Ukraine.

NATIONALITY
American

EDUCATION

2013	MA Slavic Languages and Literatures, University of Kansas, US

COUNTRIES OF WORK EXPERIENCE

Russia, Ukraine, US

LANGUAGES
English (native), Russian

RELEVANT PROJECT EXPERIENCE

2016 – Present, Digital Forensics Lab (DFRLab), Digital Lead Researcher
Leads digital research investigations at DFRLab focusing on disinformation and ongoing conflicts. Manages data collection, monitoring and analysis in #MinskMonitor project about the conflict in eastern Ukraine, with a focus on digital evidence and what it tells us about the war.

2015 – Present, Bellingcat, Lead Eastern Europe and Eurasia
Writes, edits, and translates articles for Bellingcat. Coordinates translation of all site's content into Russian with three translators through grant provided by the Open Societies Foundation (OSF). Leads training programs targeting Russian-speaking journalists, researchers, and activists specialised in digital research and verification skills. Successfully delivered two waves of workshops for over 160 journalists in Tbilisi, Kyiv, Yerevan, Bishkek, and Almaty. Developed training curriculum and guided local media to integrate best digital practices in their journalist and fact-checking work.

2013 – 2015, Bank of America, Intelligence Specialist
Responsibilities include monitoring, researching, and writing on events that affect Bank of America security or operational continuity through open source monitoring and research. Position responsibilities include monitoring for events across global space, with a specialized focus on research for Europe/Middle East/Africa.

OTHER EXPERIENCE

2016	Contributor at First Draft News.
2014	Contributor at the RuNet Echo project at Global Voices. Author of an eight-part guide for RuNet Echo providing English-language instruction on open source research on the Russian and Ukrainian-language internet.

Christiaan Triebert – Digital Forensics Specialist

Christian Triebert is investigative journalist focused on conflict, security, and development. As a member of Bellingcat and Airwars, Christian provides worldwide training in news verification and open source investigation. His works have appeared in a number of outlets, including The New York Times, Al Jazeera, Daily Beast, and Foreign Policy. In 2017, he received the European Press Prize's Innovation Award and the Prix Ars Electronica 'Golden Nica' for the entire team Bellingcat in 2018.

Christian delivered workshops about verification and open source investigation at many congresses, universities, and media organisations such as the Balkan Investigative Reporting Network, The Guardian Foundation, and ZDF.

In addition to his digital research, Christian has travelled extensively: from Afghanistan to Zimbabwe, and from the North Cape to the Cape of Good Hope. He has also conducted fieldwork as a (photo)journalist in conflict areas such as Iraq and Syria.

NATIONALITY
Dutch

EDUCATION

2015-2018	Conflict, Security & Development, King's College London Master of Arts
2013-2015	Political Philosophy, University of Groningen Bachelor of Philosophy
2010-2015	International Relations, University of Groningen Bachelor of Arts

COUNTRIES OF WORK EXPERIENCE

Austria, Iraq, Syria, Ukraine.

LANGUAGES

Dutch (native), English (proficient), German (intermediate), Arabic (elementary), Russian(beginner)

RELEVANT PROJECT EXPERIENCE

Netherlands – World Press Photo, 2018- Present, Fact Checker
Verifying the photos and captions finalists.

Multi-region- Bellingcat, 2017- Present, Senior Investigator and Trainer
Open-source investigating e.g. armed conflict, corruption, and environmental issues.

Multi-region– The New York Times, 2017- Present, Video Journalist
Working overseas with the visual investigations team on freelance basis.

UK– Airwars, 2016-2018, Geolocation Researcher
Tracking alleged civilian casualty incidents due to international airstrikes in the Middle East.

UK– International Centre for Security Analysis, King's College London, 2015-2016, Research Intern
Open-source monitoring of Turkey's nuclear program at the International Centre for Security Analysis.

Netherlands– Ukrant,2015-2016, Reporter
Investigative and human-interest stories, including reporting trips to Ukraine.

Netherlands–Radio Netherlands Worldwide,2012-2013, Blogger
Writing travelogues while hitchhiking from Europe to South Africa.

Multiregion-2011-2018, Freelance (Photo) Journalist
Bylines include Al Jazeera, The Daily Beast, and Foreign Policy (all related to digital investigations) as well as (photo)reporting trips to Iraq and Syria, published in Dutch media.

Tanya Bogdanova – Digital Strategist

Tanya Bogdanova is ZINC Network's Senior Digital Manager. Tanya's role includes digital research, audience acquisition and the development of effective cross-platform campaigns, including through analytics and conversion tracking. She leads ZINC's projects that focus on engaging Russian language audiences online. Prior to ZINC Tanya led product-specific App Store Optimisation and developed innovative projects including an Alexa Skill for the financial services firm CMC Markets. She is London-based and grew up between Latvia and London.

NATIONALITY: Latvian

EDUCATION

2011-2014 BSc (Hons), Psychology, University of East Anglia

COUNTRIES OF WORK EXPERIENCE: UK, Kyrgyzstan, Somalia, Tunisia, Latvia, Lithuania, Estonia, Bangladesh, Pakistan, India

LANGUAGES: English (native), Russian (native)

EXPERIENCE

May 2017 – Present, ZINC Network, Lead Digital Acquisition Manager

Responsible for the digital strategy across UK and Russian-language projects, including the setup of multi-platform campaigns, audience acquisition and creating tailored monitoring and evaluation frameworks to analyse the impact of digital activity.

Major projects include:

Identifying Disinformation – Client: Sensitive

- Identifying evidence of disinformation efforts in the UK across various social media platforms
- Content analysis of Russian-state owned news outlets and disinformation tactics
- Identification of bots, trolls and sock-puppets across social media platforms
- Estimating impact and reach of Kremlin-backed disinformation using Buzzsumo and SimilarWeb
- Carrying out social media listening to understand Twitter disinformation landscape using Brandwatch
- Commissioning and overseeing focus groups, and qualitative research across several sites in the UK

Mapping Disinformation – Client: Sensitive

- Understanding and mapping the Kremlin disinformation effort across the UK, US, Spain, Italy, France and Germany in the context of the Salisbury poisoning
- Identifying Kremlin-linked bots, trolls and sock-puppets across various social media platforms
- Carrying out social media listening to understand Kremlin disinformation narratives share of voice on Twitter, and key players contributing to the conversation

February 2016 – April 2017, CMC Markets, Digital Marketing Executive

Cross-platform management and implementation of campaigns, including Facebook, Pay Per Click, and programmatic advertising. Used a direct response approach to acquiring new customers and leads with the use of optimisation tactics. Lead on innovative projects such as the development of an Alexa Skill, as well as product-specific App Store Optimisation.

February 2016 – April 2017, DBD Media, Account Manager

Client facing role, managing five key Pay Per Click accounts, in a variety of sectors such as charity, retail and travel. Responsible for management, optimisation and reporting.

Jeremy Lloyd – Cyber Security Lead

Jeremy is an experienced cyber security expert who has founded and grown a business solely responsible for the cyber security of around 300 staff and 3500 clients. Jeremy has personally designed and implemented a cryptography and security framework to protect a SaaS hosting platform used by 78 of the FTSE 100, 40 of the Fortune 100, local councils in the UK, the Welsh government, NHS, and was available to the HMG on the G-Cloud.

Jeremy has a broad industry knowledge and deep understanding of software development and supporting infrastructure. Jeremy can will add value to any technology focused small/medium business struggling with any aspect of information security, validating their software development assets, the software development process, and corporate risk management. Jeremy has travelled extensively to build an effective and secure supply chain.

NATIONALITY
British

EDUCATION

1988-1990 2.1 (Hons) BSc. University of Portsmouth, Portsmouth

COUNTRIES OF WORK EXPERIENCE
Worked in: United States, Australia, Hong Kong, Switzerland, Netherlands, France, Germany, Ireland, Russia

LANGUAGES
English (native)

RELEVANT PROJECT EXPERIENCE

2017 – Present, Toro Risk Solutions, Head of Cyber & IT
As head of cyber and IT at Toro, Jeremy has overseen the implementation, audit and certification of organisations to cyber and information security standards (such as ISO 27001) and he has a strong understanding of the information security risk management, physical, technical and administrative controls, and continual improvement required for organisations to achieve the highest level of cyber security.

2017 – Present, CISO - Coded Systems Limited, Chief Technology Officer and MD
Jeremy is an advisor to small and medium technology focused businesses on software development and information security.

2017 – Present, Non-executive director, CISO – Pay Dashboard Limited
Information security leadership role and business advice.

2010 – 2017. ICSA BoardRoom Apps Limited, Executive director and lead technical architect -
Lead development of world leading Board portal package BoardPad, including apps for Apple iOS, Microsoft Windows and Android. Used by over 1,500 customers worldwide, BoardPad combines leading edge product design with top-class end-to-end security.

Responsible for all software development, the SaaS hosting platform, all systems and corporate security and corporate risk. In 2017, both ICSA Software International and ICSA BoardRoom Apps were purchased by the Diligent Group. One of only two executive directors, was key to the successful sale of the companies, on behalf of ICSA, and the subsequent successful transition to the new management team.

Russia – ICSA Software, 2012-2013 (Visited 16 times), ICSA Software, CISO/CTO
Designed the outsourcing of product development to a partner Russian cryptography company which was integrated into the BoardPad product

Australia – ICSA Software, 2009-2010, ICSA Software, CISO/CTO
Conducted client meetings including government agencies and explored the integration of all software products.

USA – Project Name, 2002 onwards, ICSA Software, CISO/CTO
Led all client engagements, conducted supplier due diligence and coordinated a complex product Penetration test by Microsoft.

Chris White – Physical Security Lead

Chris White is a proven senior leader in the public and private sectors with a high degree of cultural and political awareness. He is an experienced Risk Manager with responsibility for assuring a Plc Board that global risks were effectively managed across the Business. He acts as a senior consultant to a number of globally recognised entities in strategic risk management, security, crisis management and communication. He is also a leading international UK Government Incident/Crisis Manager and Crisis Negotiator and trainer, security vetted to the highest government level with extensive international experience in non-traditional, hostile and sensitive areas .Chris is also a graduate of the FBI National Academy, a member of the ISMA Senior Executive Leadership Programme with a global network of fellow associates and security professionals, and has extensive experience of kidnap/incidents, crisis response and investigations.

NATIONALITY
British

COUNTRIES OF WORK EXPERIENCE

UK, France, Germany, Portugal, Cuba, Nigeria, Tanzania, Kenya, Cuba, Iraq, Afghanistan, USA, Canada, South Africa, Jamaica, Hong Kong, Indonesia, Singapore, Israel, Palestinian Territories, Malaysia, Turkey, Tunisia, Egypt, Philippines, Dubai, Abu Dhabi, India,

LANGUAGES

English

EXPERIENCE

September 2017 – Present, Toro Risk Solutions, Consultant
Senior consultant into global entities in strategic risk management, policy/standard implementation, kidnap and crisis management training, security and advanced communication. Clients include (not exhaustive):

- One of the largest global financial services companies – strategic review into the Enterprise Risk Management structure across a federated model. Providing Board assurance that risks are effectively managed across the security and risk management structure
- A high-profile global sporting body in strategic risk management, global event security review, third party provider negotiation and management, reputational and travel risk management (including players) and incident/crisis response
- Major Lloyds brokers/underwriters in the field of specialist risk management
- One of the largest private sector security companies in the world – consultant response to corporate critical incidents and special risks

August 2017 – September 2017, Prudential PLC, Group Head-Operational Security and Intelligence

- Providing Board Level assurance that global Business Security risks are effectively managed
- Contributing to Group Risk Committee processes (2nd Line of Defence)
- Managing/embedding and enabling the global travel/medical security process
- Enabling Business Units to develop and embed policy and best practice
- Analysis and interpretation of the global geopolitical threat environment
- Developing the trust of EXCO and Board members, briefing and advising as appropriate
- Developing and maintaining key global/domestic corporate relationships
- Negotiating contractual agreements with third parties
- Maintaining discreet global security links across international agencies/law enforcement
- Briefing Board/Exco as appropriate
- Working with the Business and third parties to develop and enable business and intelligence

2014 – 2016, Old Mutual PLC, Group Security and Investigations Manager
Deputy to the Group Head of Security, involved in preparing board level risk papers and assessing threat and risk environment.

- Negotiating and maintaining external provider relationships
- Managing the Global Personnel Travel and Medical Security Process
- Developing and embedding the Group Crisis management Programme
- Leading / supporting Group level investigations
- Leading the Group Head Office Business Continuity Programme

- Providing advice and training to colleagues in Emerging Markets

2012 – 2014, Private Consulting

- Consulting to public and private sector in all aspects of security/investigation, risk, crisis response, hostage negotiation and communication
- Providing international advice and training to the law enforcement, oil and gas, financial and insurance markets both domestically and overseas
- Details of clients are available under separate cover on request

December 2009 – August 2012, New Scotland Yard, Counter Terrorism Protective Security Command

- Engaging with commercial/financial partners in the field of crisis management, investigation, negotiation and response, business continuity management and security
- Providing a 24-hour senior ‘on call’ response to UK government for crisis and political hostage taking overseas
- Supporting and representing the Chief Officer in key counter terrorism activities with external partners
- Developing the Counter Terrorism Technology strategy for the organisation
- Developing and implementing London’s emergency services’ response to widespread terrorist attack
- Planning and conducting tabletop exercises for businesses as part of New Scotland Yard's business outreach program, including design and facilitation of exercises designed specifically for London/UK

November 2008 – December 2009, Multinational Task Force, Chief of Operations

- Representing UK Government in a non-traditional overseas environment in a covert capacity on a multi-national task force
- Compiling a robust risk assessment for a new international initiative
- Implementation of mitigation measures in accordance with the identified risks
- Briefing up and across governments on risk mitigation strategies and implementation

Dan Williamson – Risk Management Lead

Dan Williamson works in direct engagement with humanitarian CEOs and Executive Teams through the development and roll out of a sector-specific Duty of Care system review tool and retained risk advisory support and crisis management services. Dan's risk advisory skills have been extensively developed in the last five years working with Marie Stopes International where as Head of Security he created an entirely new global security function and team. At International Location Safety (ILS) as Director of Risk Advisory, Dan revolutionised project management, risk advisory and quality assurance approaches. He established a new country programme for MSI in South Sudan and operational security management for Médecins Sans Frontières (MSF) in Iraq. He has 12 years of humanitarian and development programme experience in complex environments, at operational, management and executive levels. Dan has gained a solid sector reputation as a thought leader in security risk management having mitigated risks and crises in complex organisations and a variety of threat profile states.

NATIONALITY
UK

EDUCATION

2012-2013	MA Development & Emergency Practice, Oxford Brookes University, UK
1996-1999	BA Business Management, University of Gloucestershire, UK

COUNTRIES OF WORK EXPERIENCE

Iraq, South Sudan, Sudan, Swaziland, UK

LANGUAGES

English (native)

RELEVANT PROJECT EXPERIENCE

2012–present, Risk Management Consultant
Dan has supported humanitarian, development, human rights, peacebuilding, conflict transformation and privacy organisations to understand and achieve their legal, moral and contractual duty of care obligations to donors, fund managers, staff, consultants, partners and sub-grantees. Dan's focus and skill lies in creating simple and innovate approaches that enable organisations to effectively manage health, safety, security wellbeing and reputational risks, in a manner that fits their mission, values, governance and activities.

2016–2017, Director of Risk Advisory – International Location Safety
As one of three ILS Directors and the lead for the Risk Advisory division, Dan recruited and trained a team of seven full time risk advisors to deliver consultancy services to humanitarian, development, media and academic organisations. These services included enterprise risk management advisory, Duty of Care benchmarking, security risk management framework design, crisis management support, incident and crisis reviews, retained risk advisory support and the delivery and development of global security training packages.

2012–2016, Global Security Manager - Marie Stopes International (MSI)
Starting as a consultant to design and implement MSI's Global Security Framework, Dan was employed as the most senior member of the Global Security Team, responsible for MSI's Duty of Care, 13,000 employees, assets and reputational security in 37 countries, five support offices and the London headquarters. Accountable for the effective delivery of the Global Security Team's activities at executive, international operations, country programme and team member levels, Dan was the lead risk advisor to the Global Crisis Management and Executive Teams, Regional Directors and Country Directors.

2011–2012, Country Director – Marie Stopes International, South Sudan
Responsible for a creating a new country programme in post-independent South Sudan focusing on family planning and reproductive health service provision in a complex, insecure environment. In charge of all MSI South Sudan operations, security management, business and strategic planning processes, recruitment, external and

donor relations, new business development, programme design and implementation, policy advice to the Government and the creation of internal systems and procedures.

2011, Inter-Sectional Operations Manager & Interim Head of Mission – Médecins Sans Frontières, Iraq
Responsible for the setup and effective operation of MSF's Baghdad base serving multiple project locations in Iraq. Conducting context analysis, risk assessments and travel planning and developing and implementing enhanced security protocols and security related training. Lead for Baghdad Incident Management Team and security networking, including managing an armed private security provider.

2010, Project Manager - Population Services International, Swaziland
Responsible for setting up a USAID funded Male Circumcision programme campaign delivering access at 12 new sites. Implementation and rationalisation of PSI's human resources, technical and supply logistics systems. Specification and design of technical equipment, including a patient records database and surgical facilities. Permanent member of the Swaziland National Male Circumcision Task Force.

2008–2009, Project Coordinator, Logistician – Médecins Sans Frontières, Darfur, Sudan
Effective delivery of objectives in a large healthcare project providing multiple services to a population of 140,000, in a highly insecure environment with a team of six international, eight regional and 178 national team members. Successful management of two project evacuations during intense fighting, remote management of activities and a member of the mission closure team following the Sudanese Government's expulsions of 12 INGOs.

2007–2008, Project Coordinator/National Logistics Coordinator – Médecins Sans Frontières, Zimbabwe
Project Coordinator for a cholera intervention in a low resource, rural district. Set up of a 40 bed Cholera Treatment Centre and 19 Treatment Units in the height of the outbreak. Coordination of the Zimbabwe programme logistics across two large HIV/AIDS projects with 10,000 patients under care. Implementation of security protocols for presidential elections.

James Wilson – Legal Advice

James Wilson is a corporate and commercial lawyer with over 20 years of experience at international law firms in the City of London, executing high value, complex cross-border transactions and projects, and ranked as a leading lawyer by Chambers & Partners 2015 and 2016. He has supported the Institute for Statecraft on the UK Foreign & Commonwealth Office programme “The Integrity Initiative”, supporting NGOs and other specialist groups across Europe on defamation, data protection, commercial contracts, corporate governance and information technology/cyber security.

NATIONALITY

UK

EDUCATION

1995-1996	LPC, The College of Law, York
1992-1995	LLB (Hons) Law, The University of Newcastle upon Tyne

COUNTRIES OF WORK EXPERIENCE

UK

LANGUAGES

English

RELEVANT PROJECT EXPERIENCE

UK – 2015–ongoing, The Integrity Initiative, UK FCO, Legal Advisor

James Wilson has been advising the Institute for Statecraft on the Integrity Initiative, an FCO project to track, expose and counter the increasing level of malign Russian influence and disinformation throughout the West. James’ responsibilities included reviewing multiple articles, blogs and other publications to assess liability for libel; advising on GDPR impact on various issues and drafting organisational policies and contracts to deal with the impact; reviewing and drafting contracts with partner organisations, employees, contractors and other service providers; advising on organisational structure and constitution and providing necessary company law and secretarial services; advising on ethical and corporate governance issues including safeguarding and other policies; assisting the Institute for Statecraft in establishing distinct programmes, such as Shared Outcomes.

OTHER EXPERIENCE

- Advising Shared Outcomes, a charitable programme that works with young people from disadvantaged communities
- Advising Future Brilliance on its innovative education and training models in post-conflict areas to solve social, economic, and environmental problems, sustainably
- Advising the following charities on a pro bono basis – The Parachute Regiment Charity, The Clock Tower Fund, Airborne Assault Duxford, The Scars of War Foundation, Holy Trinity Monastery
- Advising the following high-growth start-ups on their establishment and seed fundraisings –Dribble Media Limited (mobile gaming), Adarga Limited (artificial intelligence), Parade World Limited (e-commerce), Donald Edge (jewellery), Vatcat Limited (digital VAT solutions), Blackbear Minerals Limited (nanotechnology), Footbole Limited (viral media), Lavelle Bikes Limited (e-bikes).

Deepti Sastry – Monitoring and Evaluation Lead

Deepti is a senior expert in independent monitoring and evaluation with high-level leadership roles. She has experience developing organisation-wide outcome and impact frameworks and developing monitoring and evaluation systems for projects amounting over £100m in value. Deepti has provided direct support to staff across 40+ organisations on outcome-level measurement, beneficiary participation, adaptive programming, analysis of data and use of data for decision-making. She is also experienced in researching and writing impact reports, conceptualising and reporting on value for money, and synthesising evidence.

NATIONALITY

British

EDUCATION

2015	PhD in Geography (2015), University of London
2003	MA Environment, Politics and Development, King’s College London
2002	BSc (Hons) Economics, London School of Economics
1999	B.Com (Hons) University of Delhi, India

COUNTRIES OF WORK EXPERIENCE

Tanzania, Uganda, Belize, Sierra Leone, Trinidad and Tobago, South Africa, Kenya, Somalia, Pakistan, Bangladesh, India

LANGUAGES

English

RELEVANT PROJECT EXPERIENCE

Head of Monitoring and Evaluation, Aktis Strategy, 2018-present
With Aktis, Deepti leads strategic thinking on monitoring, evaluation and learning (MEL) tools and development of systems and processes across several geographical regions and technical teams. Directing Aktis’ overall approach to M&E she has recently designed and implemented strategic M&E approaches for a wide range of projects, including in Eastern Europe.

Head of Evidence, Start Network, 2016-2018
Deepti led strategic thinking on monitoring, evaluation and learning (MEL) tools and development of systems and processes. She developed the Network’s theory of change and tools for measuring impact across 42 international organisations. She also provided technical leadership on communicating and sharing evidence for advocacy and accountability, and technical MEL training to staff located in disperse international offices

Impact and Accountability Adviser, Saferworld, 2014-2016
Provided strategic leadership on MEL for programmes in fragile and conflict-affected states, focusing on Myanmar, Nepal, Pakistan, Bangladesh, Kenya, and Somalia. Supported policy and advocacy teams to develop tools and processes to measure and communicate impact of approaches and interventions.

Performance and Accountability Adviser, Islamic Relief International, 2012-2014
Established global data monitoring system to collate evidence from country teams on change and impact. Reworked organisation-wide Quality Management Standards (IRQMS), which involved rethinking indicators and standards in line with quality and accountability best practice in the industry.

Researcher, Commonwealth Foundation, 2010-2011
Identified and establish relationships with civil society organisations in Trinidad and Tobago and Sierra Leone, training organisations on the use of research for accountability, developing workshop tools and facilitating workshops in-country.

Project Officer, One World Trust, 2007-2009
Managed project funded by the Commonwealth Foundation. Project involved working and communicating over 100 CSOs in Uganda Belize, India and the Pacific Islands. Developed methodology, conducted research, developed training tools, facilitated and moderated online forum for over 100 practitioners, managed budgets and travel, and conducted workshops for civil society on accountability.

Alex Mackintosh – Creative Support

As ZINC Network's Director of Content, Alex oversees all the creative work of the agency, from TV dramas to Facebook videos, influencer management to Instagram campaigns. He has also created several social video channels for the agency, including the eponymous ZINC, which has had over half a billion video views on Facebook. Alex previously oversaw the video production team at Breakthrough Media, where he helped find the most creative and effective solutions to some of the world's most challenging social problems. He came to communications after a 14-year career in the TV industry, where he made numerous hit shows for broadcasters such as the BBC, Channel 4, Discovery, TLC and A&E.

NATIONALITY

British

EDUCATION

2008 – 2012	PhD Humanities and Cultural Studies, University of London, UK
2001 – 2002	MPhil Latin American Studies, University of Cambridge, UK
1997 – 2001	BA Spanish and French, University of Cambridge, UK

COUNTRIES OF WORK EXPERIENCE

UK, France, Belgium, Romania, Spain, Italy, Sweden, Finland, Norway, Cyprus, Turkey, Bosnia, Georgia, Germany, Poland, Czech Republic, USA, Mexico, Argentina, Brazil, Kenya, Tanzania, Ghana, Rwanda, Morocco, South Korea, Fiji, Tonga

LANGUAGES

English (native), Spanish (fluent), French (proficient); Portuguese (basic)

RELEVANT PROJECT EXPERIENCE

2018 – Present, ZINC Network, Director of Content

As the Director of Content at ZINC Network, Alex is dedicated to helping our clients find creative and effective solutions to some of the world's most complex problems. He oversees all the creative work of the agency, from website design to influencer management, social media content to TV, radio and video production. Alex has overseen a number of ZINC projects targeting disinformation, particularly in the ex-Soviet space, including an influencer campaign in Eastern Ukraine, and another in the Baltics. He also set up ZINC's own Russian-language channel ZAG, whose mission is to challenge prejudice and misinformation in Russian-speaking countries. ZAG has been a phenomenal success – with over 5 million views a month, ZAG has become one of the leading independent Russian-language channels on Facebook.

2016 – 2018, ZINC Channel, Founding Editor

Alex created ZINC Network's own Facebook video channel, ZINC, which has become one of the UK's most successful Facebook video brands. Alex has grown the channel from zero to nearly a million page likes, with up to 50 million video views per month and numerous viral videos gaining up to 70 million views each. ZINC's mission is to promote positive social change around the world, and with a lifetime reach of 1.7 billion people, it can claim to have played a role in shifting attitudes on everything from plastic pollution to refugees.

2015 – 2016, Breakthrough Media, Executive Producer

Alex ran the TV and video production department of this global communications agency, executive producing numerous documentaries and campaign films for governments, intergovernmental agencies and NGOs, and managing a team of 25 full-time staff and numerous freelancers.

2008 – 2014, Freelance, Producer/Series Producer

During this time Alex produced, directed, shot, and edit produced, as well as series produced, numerous critically acclaimed and commercially successful documentaries for major global networks including the BBC, Channel 4, Discovery Channel, TLC and A&E.

2004 – 2008, BBC, Current Affairs, Producer

Produced, directed, shot, and edit produced numerous current affairs documentaries for the BBC.

Ziad Ramley – Digital Support

As ZINC Network's Head of Digital, Ziad oversees the strategic planning, development, and implementation of the company's digital initiatives. He manages a team of digital managers, social media editors, community managers, digital researchers, and content strategists, who have extensive experience in: tracking disinformation, social media management, audience development, and buying across all major digital platforms, SEO, social media listening, and digital publishing.

Prior to joining ZINC Network, Ziad worked in London for 11 months as a digital media consultant, providing insights, guidance, and training to major media organisations such as Conde Nast International, YLE (Finland's state broadcaster), and The National. He has also been invited to speak on various aspects of social media and journalism at The Economist, European Parliament, University of Cambridge, City, University of London, and London School of Economics and Political Science.

Before moving to London in 2017, Ziad was the social media lead at Al Jazeera English, in Qatar, for 2.5 years, where he oversaw digital strategy for the company, trained staff on how to use social media more effectively and managed a team of 8 video journalists in the social video unit. During this time, he gained invaluable experience in the monitoring and countering of misinformation.

NATIONALITY

British-Canadian

EDUCATION

2007 – 2012 BSc, General Science (Life Sciences), University of British Columbia, Vancouver, Canada

COUNTRIES OF WORK EXPERIENCE

Canada, Qatar, UK

LANGUAGES

English (native), French (basic)

RELEVANT PROJECT EXPERIENCE

United Kingdom – ZINC Network, [2018 – Present], Head of Digital

Leading and building a best-in-class digital team that helps governments, businesses, and NGOs address some of the most complex social issues facing the world today. I have overseen the planning and development of 5 cross-border disinformation projects in Europe and Africa.

United Kingdom – [2017 – 2018], Digital News Consultant

I train staff, develop best practices, and build digital strategies for news organizations. My past clients include Condé Nast International, Al Jazeera English, YLE News and The National. I worked with clients to develop effective strategies to identify disinformation and create fact-checking content.

Qatar – Al Jazeera English, [2015 – 2017], Social Media Lead

Ran digital strategy, lead an 8-person team of social video journalists, and coordinated Al Jazeera's social coverage of all major news events, such as US election night and the Battle for Aleppo. My team was responsible for the identification of misinformation and the development of social video content to counter it.

Canada – VICE Media Inc., [2014 – 2015], Associate Editor, THUMP

Wrote, edited, and commissioned articles on music, culture, and technology.

Canada – This Is Blueprint, [2013 – 2014], Digital Marketing Manager

Managed Facebook, Instagram, and Twitter accounts for company properties.

Paul Birmingham – Project Manager

With over 7 years' experience as a Project Manager, Paul has administered multi-million-pound projects for the Foreign and Commonwealth Office, US Department of State, J. Walter Thompson and the BBC. Paul's responsibilities at ZINC Network include managing staff across multiple countries, data legislation adherence, and managing complex contracts and budget requirements.

NATIONALITY

British

EDUCATION

1999 – 2003	MA (Hons) Business Studies, University of Edinburgh, UK

COUNTRIES OF WORK EXPERIENCE

Bangladesh, Chile, China, El Salvador, France, Germany, India, Iran, Israel, Japan, Lithuania, Malawi, Niger, Pakistan, Switzerland, Thailand, Tunisia, United Kingdom, United States of America

LANGUAGES

English (native), French (conversational), Spanish (conversational)

RELEVANT PROJECT EXPERIENCE

EXPOSE ToR Design, 2018, UK FCO, Project Manager
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. ZINC Network created a report which highlighted the opportunities that exist to upskill civil society organisations around Europe, enhancing their existing activities and unleashing their potential to effectively counter disinformation. Key responsibilities: forecasting and budgeting all elements of the project; negotiating and contracting freelancers; managing logistics for team members to travel across Western and Eastern Europe; liaising with internal ZINC Network departments to facilitate research and M&E.

Disinformation Research, 2018, UK FCO, Project Manager
ZINC Network was tasked to define the strategy and tactics used by the Russian state in disinformation operations (RDOs) and better measure their scale and impact. The research will identify key vulnerabilities and resilience factors to disinformation operations, shape further research into this area, and develop evidence-based and measurable approaches to reducing the impact of such operations in the future. Key responsibilities: forecasting and budgeting all elements of the project; managing contract requirements.

Navigating the Runet, 2017-18, UK FCO (collaboration with LSE), Project Manager
This project was designed to investigate whether it is possible to engage Russian audiences around social and economic themes, to reduce polarization between different Russian audiences and to advance mutual understanding between Russia and the West. Key responsibilities: forecasting and budgeting all elements of the production process; negotiating and contracting freelancers; reviewing all content for any compliance issues before publishing on Facebook.

ZAG, 2017 – ongoing, Project Manager
ZAG's daily updated Facebook page publishes specially commissioned content across Eastern Europe to bring an audience to the unique stories occurring across the region. The channel showcases original and engaging videos, which when coupled with social media marketing and promotion, helps achieve a measurable shift in the online debate around topical events as they unfold. Key responsibilities: forecasting and budgeting all elements of the production process; negotiating and contracting freelancers; scheduling editors and edit suites; reviewing all content for any compliance issues before publishing on Facebook.

Building Credible Civil Society Voices, 2016-18, US Department of State Bureau of Counter Terrorism, Project Manager
Through a multi-country training and capacity building programme, ZINC Network helped CSOs and other key influencers across each region to overcome the barriers they currently face to produce and distribute better CVE content. Key responsibilities: supporting the team's capacity building activities through managing logistics, scheduling and finance; recruiting and hiring local freelancers to assist the CSOs with campaigns.

Lyubomir Hristov - Line IT Support Analyst

A MCSE/VMware VCP5 qualified and Microsoft Certified Solutions Expert (server Infrastructure) and Microsoft Certified IT Professional fluent in English, Bulgarian and Russian.

NATIONALITY
British

TECHNICAL SKILLS

- Microsoft Windows XP /Vista/ Windows 7, Windows 8, Windows 8.1, Windows 10
- Windows Server 2003/ 2008/ 2008 R2/ 2012 /2012 R2 / 2016
- MS Office 2003/2007/2010/2013/2016
- Mac OS X 10.8/10.9/10.10/10.11/10.12/10.13/10.14
- Jamf Pro 09.10-9.101.4 / 10.0.0-10.6.2
- Lotus Notes R5, Lotus Notes Domino & Designer R 5.0.10
- VMware vSphere 5/5.1/5.5
- VMware Certified Professional 5 (VMware vSphere: Install, Configure, Manage 5X (Exam VCP5-DCV)
- Microsoft Certified Solutions Expert – Server Infrastructure
- Microsoft Certified Solutions Associate (windows Server 2012) – Charter Member
- Microsoft Certified IT Professional – Enterprise Desktop Administrator on Windows 7
- ITIL v3 Foundation certificate
- SGS – Systems and Services Certification

RELEVANT PROJECT EXPERIENCE

ZINC Network

- Providing 1st and 2nd line support to staff, assisting them with hardware, software and service issues face-to-face and remotely, always focusing on resolving issues as quickly and effectively as possible
- Working within an ITIL framework adhering to all service management principles
- Owning user problems and troubleshooting to resolution
- Prioritising requests within a Helpdesk system and maintaining an audit trail of customer communications
- Proactively managing a starters and leavers process, preparing equipment, accounts and access permissions
- Participating in employee training and educating users on procedure, processes and inductions
- Performing configuration of devices, systems and managing upgrades within a controlled change management environment
- Asset management and device deployment
- Supporting company presentations and proactively maintaining company AV
- Researching and risk assessing applications and software to advise the business on safe products for use
- Support of company telephony and mobile phone contracts
- Log and keep track of laptop repair
- Contributing to the documentation of all aspects of IT service delivery

Pretty London Limited IT Support Analyst / Freelance

- Providing an IT Support for various shops (Mascaró/Pretty Ballerinas) around London
- On site /email/phone/chat/face to face and remote support via Team Viewer, DameWare and Remote Desktop Connection
- Acting as the first point of contact for all IT & Technical Queries.
- Maintaining a log of all incidents into TopDesk and making sure all incidents were logged accurately with as much detail as possible to ensure that all incidents be resolved effectively by me or 3rd Line support engineers
- Installation/Configuration of standard PC’s (workstations)/laptop build
- Hardware Support of PCs, Laptops and peripherals
- Diagnosing & resolving hardware, software & end users problems.
- Escalating any unresolved/unsupported issues in a timely manner to the appropriate teams
- Migration of computers/laptops from Windows XP to Windows 7 and Windows 7 to Windows 8
- Supporting: MS Office 2003/2007/2010, Retail Excellency

Other Short-Term Technical Assistance Staff Bios

RUSSELL PEACOCK – GRANTS MANAGER

Russell provides leadership, quality assurance, implementation and technical assistance to a portfolio of UK grants programmes. He has been responsible for managing the successful delivery of EU Communications contracts and framework assignment for DG EAC and DG JUST, for supervising and managing communication activities, developing proposals and action plans, sourcing and appointing appropriate experts, liaising and coordinating with clients, partners and subcontractors in order to plan and implement activities, quality control, financial management and reporting.

CHARLOTTE BECKETT – RESEARCH LEAD

Charlotte is a strategic planner and consumer behaviour specialist, with a MSc in Consumer Psychology. She has over 17 years' experience in developing strategies from insight to implementation and have worked with a range of sectors including government, NGOs and not for profit, financial services, FMCG, tech and healthcare. Her expertise includes: qualitative and quantitative research (design and delivery), consumer behaviour, insight and trends, brand strategy and brand experience design, digital strategy, creative strategy (including content and communications) and customer journey development.

Advisory Board Bios

NEVILLE BOLT - DIRECTOR, KING'S CENTRE FOR STRATEGIC COMMUNICATIONS

Neville is one of the world's leading experts in strategic communications, and currently holds the position of Director of the King's Centre for Strategic Communications (KCSC) in London. He is also the Editor-in-Chief of NATO's peer reviewed academic journal Defence Strategic Communications, and an Associate Fellow of the International Centre for Counter Terrorism (ICCT), The Hague. He will bring his wealth of experience in strategic communications and disinformation to the project, advising on all elements of strategic approach, delivery and measurement and evaluation.

PETER POMERANTSEV – INDEPENDENT CONSULTANT

Peter Pomeransev is a Senior Fellow at the Institute of Global Affairs at the London School of Economics and Political Science. He is the director of the Arena Programme, a think tank dedicated to overcoming the challenges of digital era disinformation and polarisation. His book on Russian propaganda, *Nothing is True and Everything is Possible,* won the 2016 Royal Society of Literature Ondaatje Prize, was nominated for the Samuel Johnson, Guardian First Book, Pushkin House and Gordon Burns Prizes. It is translated into over a dozen languages. He has testified on the challenges of information war and media development to the US House Foreign Affairs Committee, US Senate Foreign Relations Committee and the UK Parliament Defence Select Committee. He is a columnist at the American Interest, and writes for publications including the Financial Times, London Review of Books, NY Times and many others.

MILICA PESIC - EXECUTIVE DIRECTOR, MEDIA ADVISORY INSTITUTE (MDI)

Milica Pesic is Executive Director of the Media Diversity Institute (MDI), a non-for-profit London-based international organisation specialized in inclusion of diversity through media and media education. Milica has designed and supervised multi-national, multi-annual diversity media development programmes in Europe, NIS, MENA, South Asia, the Sahel, Sub-Sahara, West Africa, China and Cuba. A journalist by profession, she has reported for the BBC, Radio Free Europe, the Times HES, TV Serbia and other media. She holds an MA in International Journalism from City University, London.

GRAHAM BROOKIE – MANAGING EDITOR, THE ALTANTIC COUNCIL – DFRLAB

Graham Brookie joined the Council in May 2017 as managing editor of the Digital Forensic Research Lab. Before, he served in various positions at the White House and National Security Council. His most recent role was as an adviser for strategic communications with a focus on digital strategy, and audience engagement. Previously he served as the adviser to the assistant to the president for homeland security and counterterrorism, the president's top aide for cybersecurity, counterterrorism, intelligence, and homeland security issues. He also worked in the East Asia, Middle East, and North Africa directorates at the National Security Council.

BEN NIMMO - SENIOR FELLOW, INFORMATION DEFENSE, THE ALTANTIC COUNCIL – DFRLAB

Ben Nimmo is the information defence fellow with the Atlantic Council's Digital Forensic Research Lab. He is an analyst of defence and international security, specializing in patterns and trends on disinformation and hybrid warfare. From 1999 to 2011 he worked as a writer and journalist throughout Europe, including five years in Brussels covering EU and NATO issues for Deutsche Presse-Agentur. In 2011 he joined the NATO press office. His duties involved expertise in fields including NATO-Russia and NATO-Ukraine relations, partnerships, deterrence, and conventional and missile defence. He is a senior fellow of the Institute for Statecraft in London, an associate scholar of the Centre for European Policy Analysis, and is fluent in languages including French, German, Russian, and Swedish.

JESSIKKA ARO, INVESTIGATIVE REPORTER, YLE

Jessikka Aro is an investigative journalist with the Finnish Public Broadcasting Company's cross-media product Lie Kioski. Aro specialises in research into Russia, extremism and information war. She won the Bonnier Journalism Prize in 2016 for her research about pro-Russia trolls in Finland. At the moment she is investigating and writing a book on how Russia-connected activists troll, hack and stalk civilians internationally.

1.5 Concept and Methodology

The consortium brings together ZINC, Aktis Strategy, The Institute for Statecraft, Bellingcat, DFRLab and the Media Diversity Institute (MDI) to offer market leading capabilities in understanding, monitoring and countering state backed disinformation to not only expose disinformation but also to undermine the credibility of the networks behind it, help build resilience to it, and build a more sustainable sector over the next three years.

Our proposal offers: • **deep geopolitical and practical understanding of Kremlin's disinformation** activities across Europe • both **in-house teams and existing networks of CSOs, activists, media organisations and practitioners** able to effectively counter disinformation at pace and scale • an operating model that **adapts to local contexts** and **iterates strategy and tactics based on insights** from ongoing monitoring and evaluation • a proven approach to **building and managing networks** in a way that optimises delivery whilst sustainably building their **capacity** through co-creation and embedded learning and focused core funding; and • **a robust approach to risk management and safeguarding** based on experience delivering discreet high-security, high-value projects for government clients including the FCO and the Home Office.

Upskilling to Upscale: Understanding the Problem

We understand that state backed disinformation is not just about propagating false or misleading information, but more broadly about manipulating the information environment to further anti-democratic objectives including undermining the credibility of mainstream media, growing cynicism and distrust towards democratic institutions and processes, increasing polarisation between communities, and destabilising international alliances. The tactics used by the Kremlin and other actors to achieve these ends are adapted depending on the context and objectives. For example, they can not only include the dissemination of false narratives but also the weaponisation of wholly or partially true narratives. Therefore, **to identify disinformation we need to genuinely understand the adversaries' objectives in each specific context and the vulnerabilities of the target audiences they seek to influence.**

The Kremlin harnesses the influence and credibility of multiple actors within a complex ecosystem which may contain for example, the mainstream media, fringe groups drawn from the far right or left, commercially motivated advertisers and even other malign state actors. **To effectively expose and counter disinformation we need to build networks of partners who have influence at key points throughout the ecosystems which our audiences exist within.**

Disinformation is often at its most effective when it affirms the existing attitudes, beliefs, fears, and prejudices of its target audiences. This means that those most vulnerable to disinformation are those who are already disaffected or mistrustful of 'mainstream' opinion. Myth-busting or fact checking content these audiences are engaging with, often only further entrenches their views. **To be effective any attempts to counter disinformation must involve a broad suite of approaches, which go beyond fact checking or myth busting**.

In some countries, governments are intertwined with Russian state disinformation efforts, either in direct support or in passive complicity. In others, influential sectors are directly invested in the Kremlin's efforts through cross-cutting threats such as organised crime, corruption or far right politics. The threat therefore varies not only region to region and country to country, but also within countries. **Expose activities must take place within a framework that recognises, identifies and adapts to the complex geopolitical factors active across the countries targeted and the diplomatic sensitivities that this entails.**

A growing number of Civil Society Organisations (CSOs), activists, academics, policy makers and media organisations are emerging across Europe with the basic skills and motivation to expose the Kremlin's information operations. However, they are often working in isolation, responding tactically to a narrow aspect of the threat, and have limited resource or capability to design content that delivers real impact. Moreover, they face extensive challenges and threats to their operations which restrict them from reaching their full potential. These include a lack of expertise and tools to deliver high-quality open source research, a lack of ability and support to conceptualise and deliver public facing campaigns that genuinely engage the audiences actually vulnerable to disinformation, a lack of access to grant funding and core resources, and an absence of security frameworks and legal training to run streamlined and low-risk operations in the face of significant threats. **To unleash the capability of these actors to sustainably challenge disinformation requires a grassroots-led approach.**

Our Approach and Operating Model

We will mobilise a Network Hub based in London, led by an experienced Project Director, consisting of a small, agile team with core competencies in digital network analysis and targeting; open source (OS) research; journalistic ethics, strategic communications and campaigns; PR and crisis communications; cyber security and risk; and libel, vexatious litigation and compliance. The Hub will be augmented by a wider pool of experts, provided by our project partners, who can be drawn upon for specialist skills, specific training packages, or advice as needs arise. This offers flexibility and value for money by only deploying resources that are actually required.

Our approach is highly localised, based around regional clusters of actors who can collaborate to effectively undermine the disinformation ecosystem in their respective areas and engage audiences most vulnerable to disinformation. Regional Network Managers – experts in countering disinformation with deep understanding of local dynamics and Network Members themselves - will be the primary interface between regional clusters of organisations and the Hub. They possess in-depth understanding of the local dynamics, opportunities, threats and needs of Network Members. They will be responsible for working with clusters to develop both detailed organisation specific plans and comprehensive regional strategies for countering disinformation. They will then design bespoke capacity building and core support packages to support Network Members to deliver against these strategies and plans, drawing on resources from the Hub and also the wider pool of experts as required. Network Managers will work with their clusters to measure impact and their progress, adjusting both strategies, resources and capacity building support as required. This approach to the Network puts those with the greatest and most current contextual knowledge in the driving seat as 'commissioners' of capacity-building and campaigning support.

Whilst providing ongoing training, mentoring and hands on support to all organisations in the network we will focus resources and support to Network Members who are operating in priority countries, or have reach into key identified target audiences, to deliver high impact counter disinformation activities at pace and scale whilst measurably increasing their capacity and sustainability (discussed in section 1.8). Our approach to capacity building includes not only formal training but also intensive mentoring and 'learning through doing'. For example, our project includes two of the world leading OS researchers, provided by Bellingcat, who will embed with Network Members for up to two weeks at a time to work alongside their teams to expose disinformation and in doing so transfer not only the skills they need to deliver but also help them construct the systems and processes to do so sustainably (see section 1.8).

Although the activities of specific Network Members will remain discrete, The Hub will be public facing, openly presenting itself as a project that brings together actors with a variety of expertise and interests in promoting media integrity across Europe. The positioning of the project in the broader media development and integrity sector is essential to help mitigate reputational risks both to the FCO and to safeguard the interests of Network Members (see section 1.11).

We have prioritised monitoring and evaluation throughout the project, by supporting Network Members to conduct ongoing evaluation of their activities and centrally measuring the impact of the project's activities amongst vulnerable target audiences. We have developed a number of feedback mechanisms to ensure that the insight gathered is used to iteratively adjust our strategy and tactics and refocus resources as required to maximise impact (see section 1.12). The project will be overseen by an advisory committee comprising some of the world's leading experts and organisations in countering disinformation who will help guide the project against specific and measured KPIs whilst ensuring we engage key senior stakeholders from all sectors. ZINC will provide a secretariat for the project, offering the client a single point of accountability and contact for all aspects of project delivery and management as well as effective oversight of strategy, activities and risk.

We will underpin activities with a robust risk management framework which takes as paramount the safeguarding of Network Members and other stakeholders as well as the potential reputational risks to the client. We have built in extensive capacity building and support for Network Members, and also a comprehensive risk identification, monitoring and response mechanism, which ensure that risks are identified and responded to in a proportionate, timely and effective manner (see sections 1.2,1.3 and 1.11).

CASE STUDY: Building a counter disinformation network. In 2015 The Institute for Statecraft launched the *Integrity Initiative* to track, expose and counter the increasing level of malign Russian influence and disinformation throughout the West, establishing networks across nine European countries, with a further 14 on track to be fully operational by the end of March 2019. As part of this work the Institute has partnered with over 43 NGO's and other local specialist groups across Europe, building a grass-roots campaign and developing a profound understanding of the challenges faced by those at the forefront of exposing and countering Russian disinformation in Europe.

Pillars of Activity

Our activity is designed around five pillars: **BUILD - SUSTAIN - TRAIN - CAMPAIGN - SCALE**. ***Build*** focuses on creating an agile, high impact Network that can effectively counter disinformation in target countries, addresses the lack of coordination between organisations and the isolation they experience by creating groups for knowledge sharing and peer-to-peer support, and connects organisations with the local experts and resources they require; ***Sustain*** overcomes the resourcing challenge by providing core funding through a grants mechanism, developing organisational business plans and helping them to access third party funding opportunities, and support to help Members put in place governance structures, operating procedures, risk management approaches and basic legal and insurance requirements to increase organisational sustainability; ***Train*** will ensure Members are upskilled and mentored in best practice in exposing and countering disinformation from OS research through to viral video production and digital targeting as well as cyber security, libel and data compliance; ***Campaign*** will enable them to increase the pace, scale and quality of their outputs and activities, targeting specific vulnerable audiences through a process of campaign co-creation and project specific funding; ***Scale****, which is outside of scope of the ToR,* but integral to our Network Model*,* will link the organisations across borders, establish a shared set of standards and protocols and feed learnings up and out to wider stakeholders including policymakers and tech companies. Underpinning these activities are rigorous monitoring and evaluation, risk management, and quality assurance procedures.

CASE STUDY: Building local capacity while achieving shared outcomes. In 2012 ZINC pioneered a network management model for the Home Office's Research Information and Communications Unit (RICU), bringing together over 60 organisations to increase their ability to credibly campaign against extremism. Through a process of co-creation, organisations were upskilled to develop organisational communications strategies as well as to deliver campaigns on topics including cyber safety, safeguarding, and humanitarian crises. ZINC has since adapted this model based on lessons learned and has developed network hubs in Bangladesh, Somalia, and Pakistan supporting a total of 50 organisations to engage over 10 million people.

BUILD: *Creating an Agile and Effective Network*

The Consortium has existing relationships with all the organisations identified by the FCO, as well as hundreds of other actors including social media influencers, NGOs, digital activists, media organisations and policy makers across Europe who we have already vetted and trained to counter disinformation effectively. Starting with the 56 organisations identified in the ToR we will use these relationships to design a Network that meets the following criteria (1) has reach into all aspects of the disinformation ecosystem, (2) has influence and reach into all key target audiences, including not only media and policy makers, but also those most vulnerable to disinformation e.g. fringe media, far right or far left groups, (3) has coverage in key geographic areas, (4) has proven capability in and commitment to countering disinformation and, (5) has the potential to scale their activities. We will use a tiered system to focus core support on specific Network Members, in key priority countries who can deliver measurable impact, helping to drive value for money and impact. We will work with our Network Managers, to identify new organisations with new ideas and approaches, for example Eurus (Estonia), Sho Tam (Ukraine) and the Georgian Institute for Strategic Studies (Georgia). Further activities under the BUILD strand will include ongoing coordination of activities, facilitating peer-to-peer learning amongst Network Members, and building a community across Europe of actors working to counter disinformation through a secure online communication system and regional networking / training events each year. These are discussed in depth in 1.9. These tiers will

PRIORITISING SUPPORT: Using tiers based on geography and impact. We will establish a tiered system based on the FCO's regional focus and an impact factor. Activity in the SUSTAIN (including core financial support), Train, and Campaign strands will all be allocated according to these tiers. This will focus efforts on a core cohort, able to achieve 'quick wins' in the most urgent contexts. Rather than countries and organisations being fixed, these tiers can shift as the project and the geopolitical climate evolves. Tier two, operating in a wider geography, will enable the focus of the network to shift quickly if necessary and in response to disinformation flashpoints such as elections. A full list of tiered organisations will be presented to the FCO for discussion at project inception.

- ***Tier One: High Impact, 12 Priority Countries*** *(40% of organisations) anticipated to be drawn from the Baltic States, Moldova, Georgia, Ukraine, Belarus the Visegrad Four, and the Western Balkans.*
- ***Tier Two: High Impact, Rest of Europe*** *(30% of organisations)*
- ***Tier Three: Low Impact: 12 Priority Countries*** *(30% of organisations)*

form the basis for prioritisation across all Network activity. With a large number of organisations (up to 60 at any one time) it is essential that Network Managers can focus their time and resources in order to achieve maximum impact. Core funding, training, and the ongoing mentoring and support that Network Managers provide to their clusters will all be allocated on this basis.

SUSTAIN: *Providing Network Members with the core resources and support to grow*

Network Managers will work with each organisation in their cluster to develop a tailored Organisation Sustainability Plan. This plan will assess each organisation's income, staffing, the spread of commercial income vs. grant funding, and how they can shift their business model to increase sustainability over the three-year period of implementation. This will include training in grant proposal writing, budget design, monitoring and evaluation, and identifying opportunities. Priority organisations will be able to access grant funding to implement this plan (see below). Additional activities in this pillar are focused on building organisations resilience to operating in a high risk environment including legal support to ensure they are better protected from vexatious litigation, cyber support to ensure deterrence, access to a content reviewer to mitigate against libel accusations, a fund for public liability insurance for up to 20 high-risk organisations (to ensure they have resources to respond to vexatious litigation), a cyber reporting function to monitor the network for attacks, and personal safeguarding training. The SUSTAIN pillar also offers a rapid response function, deploying a team of specialists to provide support in the event of a crisis, whether internal or due to hostile external activity.

PRIORITISING SUPPORT: Core grant funding We will implement a flexible grant funding mechanism with criteria based on impact and success for core organisational funding. This could include staff costs, operational overheads, or equipment. Our grant fund will be allocated £900,000 over three years. A large percentage of this funding will be allocated to Tier One organisations; the rest will be allocated across other organisations. This will be overseen by a dedicated Grants Management Team, provided by Ecorys, who will ensure compliance, conduct monitoring, and submit monthly reports on spend and activities conducted. The grants mechanism will ensure full transparency of process and provide accountability to the FCO for how and where investments are being made, in line with the priority tiers already mutually agreed upon.

The grants timeline and structure will be flexible and can be refined with the FCO at inception and each year as we learn more about the needs and strengths of Network Members and of programme priorities. Initially, we propose one funding call to take place in early 2019, providing an opportunity for a "Quick Win" investment in Network Members and projects that are investment ready. In subsequent years we will operate two to three funding calls, with two concurrent routes, one for small grants and one for large grants. The small grants route will be simplified with shorter turnaround times and light touch assessment and audit processes to allow members to apply for funding for short or discrete pieces of work. We recommend that the small grant fund is in place for sums up to £5,000.

TRAIN: *Measurably increasing the capacity of the Network across key competencies*

All training and capacity building activities will be developed jointly between the Network Managers, with the most knowledge about the local dynamics, organisation's objectives and needs, and the Network Members. Training will be locally adapted, flexible, and tailored to each organisations' needs. It will leverage the core expertise in the hub as well as a pool of experts with specific skills and **will focus on upskilling organisations in the core competencies required to tackle disinformation**. In Year One, three training sprints in the form of four-day intensive workshops will be hosted in five regions, open to all Network Members serving to increase buy-in and basic skills, reduce isolation, and facilitate peer-to-peer learning. These will cover:

1) Sustainability: physical safety, cyber security, risk management, safeguarding (Jessikka Aro) business development (linking with activities in the SUSTAIN pillar detailed above),
2) Research and Data Gathering: digital forensics training (Bellingcat), investigative journalism, ethical and legal standards of journalism (MDI),
3) Campaigning: PR, Crisis Communications, video production, audience segmentation and targeting, campaign planning. At the end of year one a needs assessment process will establish the specific skills gaps for year two and three. In addition to the sprints below, organisations in Tier One will also have access to a host of other tailored training opportunities, including bespoke training sessions and online courses.

Priority Network Members will then be able to benefit from bespoke packages of intensive, hands on mentoring and support to ensure priority organisation learn through doing alongside leading experts. Network managers will be responsible for designing these packages with their clusters but they could include: our two Bellingcat OS research experts spending up to two weeks per year embedded with each of organisation training their team on OS research by working alongside them on expose activities; our in-house digital expert training them to map their target audiences online using leading social media mapping and listening tools, build targeting profiles, utilise social media advertising techniques to disrupt and divert vulnerable audiences away from disinformation; support from ZINC's creative and production team to build organisations capacity to turn expose research into effective products and content which are targeted to specific audiences e.g. viral video, imagery and gifs. *In addition to these training and mentoring services, and access to consultancy from experts listed in the technical pool,* Network Members will have access to a host of other services and offers including: • Three users per organisation for a secure information sharing portal (*MS Office*) • Access to a campaign and production fund • Access to a social media marketing fund • £1,500 allocation for business related insurance per Network Members for the top 20 high risk organisations • Access to grant funding for core operational and overhead costs • Access for 10 members to access professional tracking software • Access for all members to digital analytics software including *Tweetdeck* and *CrowdTangle* • Enrollment in an industry-leading e-learning cyber training programme.

CASE STUDY: Upskilling in digital forensics skills through embedded learning. Since 2014 Bellingcat has delivered training for individuals from over 350 organisations, including the International Criminal Court, the United Nations, and major human rights NGOs such as Human Rights Watch. Bellingcat is considered the leading organisation in the use of online OS investigation, best known for its groundbreaking work on the downing of Malaysian Airlines 17 over Eastern Ukraine in 2014. Bellingcat has also actively engaged with and built online and offline communities. Embedded learning is key to Bellingcat's approach, whereby a trainer with linguistic capability embeds with an organisation for a process of two months and works alongside a team on a specific research project. This enables an organic skill transfer and ensures learning is consistent throughout all points of the research process from beginning to completion of an investigation and the sharing of its findings.

CAMPAIGN: *Delivering an uplift in the pace, scale and quantity of expose outputs*

The scoping revealed that organisations need support to increase the quality and quantity of outputs and to reach wider audiences. The campaign strand will develop the Network Members' skills to amplify their messages and the impact of their research outputs. In addition to the network wide campaign training delivered in training sprint three, Network Members in Tier One will be able to apply for support from the Hub to deliver specific research or communications activities, through a ring-fenced fund consisting of £100,000 per year funding, £50,000 per year in social media marketing spend, and £50,000 per year in creative, design and campaign support to ensure the quality of outputs. This will be underpinned by principles of editorial integrity and independence, as organisations are supported technically but retain ultimate control over what they publish.

To increase Network Members' reach and impact we will support them to not only conduct specific campaigns but to better target their content to their intended audiences and engage with local, regional and international press on an ongoing basis. Network Managers and The Institute for Statecraft's experts will help Network Members to partner with journalists in their region as well as academic institutions in order to create a scaled and sustained, yet rigorous, flow of expose content across all aspects of the media in line with the regional and audience specific strategies developed by Network managers and their clusters.

Going beyond the ToR, we propose using the Network to deliver a rapid response function, by coordinating members' activities and resource to respond to pertinent anniversaries or events, such as the annexation of Crimea or local elections, or at flashpoints of disinformation. The Network Managers would coordinate this activity in their clusters accordingly, yet informed by a centralised strategy under the direction of the Project Director who will work closely with the FCO.

SCALE: *Connecting governments, media, tech platforms and grassroots implementors around standardised protocols and a shared vision*

If the sector responding to Kremlin-backed disinformation is to scale and flourish then it is vital that standards, norms and protocols are developed, implemented, and widely understood. If this is achieved then the sector can come together in a united fight against Kremlin-backed disinformation, no longer hampered by the same level of risk. This strand will foster greater collaboration between Network Members, governments, tech companies and the media development sector through a stakeholder engagement programme that ensures learnings are shared and disseminated. Insights from peer to peer networking and insights drawn from the monitoring and evaluation cycle, will feed into policy recommendations. By facilitating cooperation through joint activities, the project will contribute to breaking the cycle of mutual recrimination between governments, media and tech platforms; an atmosphere that undermines cooperation and feeds the Kremlin's efforts to undermine faith in democratic institutions.

The SCALE strand will also encourage other donors to provide additional financial resources to the Network and the wider sector. The role of DFRLab in helping to achieve this will be vital, as they will secure the support and buy in from the tech companies including *Facebook* and *Twitter.* ZINC also has strong relationships with both the EU and US Government bodies (including the GEC, USAID and EUCOM) responsible for supporting counter disinformation activities, and working under direction from the client we will hold a series of discrete briefings in order to encourage them to leverage funds.

In addition to **BUILD - SUSTAIN - TRAIN - CAMPAIGN - SCALE,** the project will have three cross-cutting functions: Risk Management, Monitoring and Evaluation, and Quality Control. These are discussed in more detail in sections 1.11 and 1.12.

The Consortium

The consortium is led by ZINC who will provide the FCO with a single point of accountability and contact for all aspects of project delivery and management. ZINC will be supported by a range of partners, who, through the Advisory Panel will help guide project strategy, deliver key work streams and oversee and quality control of all deliverables. This management and accountability structure is addressed in 1.6.

ZINC has delivered projects for clients including the FCO and the State Department, that monitor, track and counter the Kremlin's disinformation activities. ZINC has also managed complex networks of stakeholders, including supporting over 50 counter extremist organisations in the UK for RICU, and delivering network-driven counter messaging campaigns across some of the world's most challenging territories, including Iraq, Somalia and occupied parts of Ukraine. ZINC has managed multitasking contracts from governments, including a £15, 000, 000 per year contract with the Home Office and a UN contract in Somalia of £8,000, 000 per year over five years.

The Institute for Statecraft is a non-partisan think (and 'do') tank, which has successfully delivered a variety of programmes, including in partnerships with HMG and NATO. The Institute has deep expertise in Russian and Soviet affairs; on Soviet military doctrine, and its use of co-ordinated 'hybrid' conflict; and specifically, the theory and practice of disinformation, including its recent spread into social media.

Aktis Strategy is a global consulting firm that provides advisory, management, and monitoring and evaluation (M&E) services for conflict, security, and governance projects to DFID, the FCO, and Home Office in Lebanon, Tunisia, Horn of Africa, and Northern and Eastern Europe, amongst others. Aktis leverages local expertise working closely with local partners, applying flexible, adaptive tools, and innovative research and evaluation methods.

The consortium will also work with a number of resource partners and consultants who will (1) support the delivery of specific activities (2) join the project Advisory Panel (3) get buy in from relevant sectors.

DFRLab are global leaders in tracking disinformation efforts in the online space. DFR convene senior policy makers and train journalists around the world to respond to this disinformation. They have built a network of tech companies, global political leaders and policymakers working to establish norms and protocols for the sector including standards for open source research and attribution scales.

Bellingcat exposes Kremlin information interference through forensic digital investigations; including the shooting down of MH17. Bellingcat will train Network Members in open source research and social media investigation, developing a cadre of organisations with a digital forensic skillset using open source research tools.

The Media Diversity Institute (MDI) has supported media integrity, training journalists and promoting media development in Eastern Europe since 1997. Their experience promoting high quality journalistic standards and freedom of speech across traditional media will ensure the consortium maintains a strong focus on the legal and ethical challenges prevalent in being a journalist under attack by the Kremlin.

Toro Risk Solutions provide cyber, physical and personnel security for clients worldwide. They have developed over 50 security risk management frameworks for NGOs working in the humanitarian, development, human rights, peacebuilding, conflict transformation and privacy sectors.

Ecorys are a European research and consultancy company and will oversee the grants mechanism. They have extensive experience managing grant components for government agencies and are a supplier on all Lots of the Cabinet Office Grants Management Framework RM949.

We may also work with **Arena at the London School for Economics** (LSE) to deliver discrete research projects, but they are not a member of the consortium. Peter Pomeransev will sit on the steering committee in an individual capacity rather than as a representative of the LSE.

1.6 Approach

Proven Contract Management

ZINC Network (ZINC) has experience of managing large, complex projects across the globe, as well as managing a large network of institutions, NGOs, media partners and digital influencers across Europe, including a £15, 000, 000 per year high security project based around a civil society network on behalf of the Home Office and $3, 000, 000 per year on managing influencer networks across Eurasia on behalf of the US Government. This is a complex and high-risk project which requires an open, trusting and flexible relationship with between supplier and client. At project mobilisation we will develop a detailed project plan including milestones and KPIs, a detailed risk register and financial and contractual protocols to be agreed with the FCO contract management team.

As a prime contractor, ZINC is bringing together a consortium consisting of some of the world's leading organisations operating in this sector whilst offering the FCO a single, accountable point of contact which operates to the highest standards of financial, risk and project and subcontractor management (discussed in detail below). Our Project Director will offer a single point of contact for all issues related to the contract, whilst ensuring that the FCO has clear points of contact throughout the project team (in terms of specific geographies, specialisms, and technical areas) should they require direct access. The Project Director will report directly to our Managing Director, Louis Brooke, ensuring that the FCO has a clear escalation process directly to the Project Board. The Project Director will be supported by an Advisory Panel which includes leading experts from academia, media, communications and specialists working on this problem set, which will meet quarterly to review project progress against its KPIs and provide detailed input into its forthcoming activities and priorities.

Client Reporting

Clear and consistent client reporting is essential to maintaining a strong and productive relationship with the FCO on this project and to ensure it has oversight of the projects strategic progress. Precise reporting requirements will be agreed with the FCO but we envisage will include: weekly status reports covering key outputs delivered by the Network, real-time generated data e.g. online reach and engagement, an updated risk register, plus any notable events; monthly narrative reports with impact analysis of key activities undertaken by the project, recommendations for changes in priorities and strategy over the next month, detailed review of risk registers and reports on any grants awarded; quarterly reviews providing a holistic and in-depth look at the progress of the project against its strategic goals and KPIs, and a forward looking strategy and implementation plan for the next quarter.

Quality Management

ZINC will ensure a quality management process for this project that is consistent with our work for FCO and other client projects, and with the principles of ISO 9001. Our quality management approach will be overseen by our Project Board, including oversight from our Advisory Panel and management staff within the team. Our general approach to quality management will involve the following:

- **Quality Assurance:** We will establish standards, processes and regulations for all project staff to abide by and assess quality assurance based on compliance with these elements. On this project, such internal compliance checks will be carried out for both ZINC staff and our Subcontractor staff
- **Deliverable Review:** In addition to the six days per year set aside for the advisory committee to meet and discuss contract performance, amongst other things, we will establish appropriate and regular stages of review. These review stages will be overseen by the Project Director, working directly with the Senior Network Manager, team peers, short term technical assistance experts and our experienced Consortium Partners. The review will assess both the Consortium Partner 's deliverables and the Network Member deliverables.
- **Performance Achievements:** This will include reporting against our Key Performance Indicators, obtaining FCO feedback and also soliciting feedback from Network Members. Specifically, we propose that our Project Director arranges a monthly face-to-face catch-up with the FCO's Counter Disinformation and Media Development (CDMD) team, as well as provide a weekly written report on achievements, as noted above.
- **Peer to Peer Quality Enhancement:** Our proposal encourages Network Members to share best practice and learning from one another, in order to enhance the quality of the outputs and programme objective.

- **Quality People:** ZINC will provide the right people on the right jobs by using best-practice recruitments, in-depth knowledge of the sector, development and retention processes and adherence to our Code of Conduct.

Financial Accountability and Reporting

The Finance Team produce accounts on a monthly basis, applying rigorous checks and controls in order to detect errors in a timely manner. Cost Managers (CMs) track and forecast at the project level with regular reconciliation to the finance system (Sage Accounting) for accurate spend. On contract signature a project budget is entered into the cost manager system and a unique project number is granted. Cost coding and categorisation is allocated to facilitate reporting. Supplier invoice approval and client invoice generation is produced according to approval levels and contract billing cycles respectively. **Accountability**. For fraud prevention, all Project Managers (PMs) are required to answer four questions on cost expenditure to identify whether costs are 'allowable', 'allocable', 'reasonable' and 'necessary'. CMs test costs against PM justification and audit expenditure monthly. We also maintain role-based access to all systems and data and have independent auditors for annual inspection of costs and systems. **Forecasting**. Through timesheets and regular meetings, the team are able to forecast revenue and project costs. PMs work with the accounts management team to track and highlight any aspect of the contract that is underperforming or scope-creep to manage project costs for maximum Value for Money.

In order to ensure Value for Money (VFM), ZINC applies two key principles as follows: (1) maintaining "internal" value – the economical and efficient delivery of services in relation to their costs in order to deliver effectiveness (e.g. competitive staff fees through benchmarking; local consultants; strict control of reimbursable expenses and in-house capability) (2) ensuring "external value" – the efficiency and effectiveness of interventions in achieving results (e.g. milestone and performance-based payments; post-contract sustainability of interventions; leveraging local stakeholders to maximise impact). We will facilitate and supervise others, including our sub-contractors (SCs), to maintain VFM principles throughout the life of the contract, whilst managing potential cost implications due to the uncertain nature.

Internal Fraud and Corruption Policy: ZINC has harmonised our own established internal fraud processes with DFID's 2011 ICAI report to ensure we meet and go beyond government best practice. Our HR lead acts as our internal Compliance Lead to provide advice, training and awareness-raising to staff on internal fraud measures and reporting guidelines. Segregation of duties is imperative to prevent internal fraud. We also maintain role-based access to all systems and data and have independent auditors for annual inspection of costs and systems.

Monitoring and Managing Subcontractor Performance

ZINC maintains healthy supply chains with 70+ subcontractors on 10 projects in 12 countries (including across North and East Europe). We create a transparent environment with our subcontractors where disputes are proactively resolved in a respectful manner. Following internal best practice guidance, our Project Director will meet with our main implementing consortium partners, Institute of Statecraft and Aktis, on a weekly basis and with our resource partners, Bellingcat, Media Diversity Institute (MDI) and DFRLab, on a monthly basis, with periods during the contract where the frequency of meetings will need to be scaled up or down, depending on the amount of work being undertaken by the subcontractor at the time. We will also send weekly emails to all subcontractors to provide them with key updates to the project and any performance messages.

All sub-contracts will incorporate well-defined procedures for dealing with poor performance. If the FCO files a complaint that concerns – in whole or in part – the performance of a subcontractor, the Project Director will launch an investigation into this complaint with the full support of resources required from the ZINC Senior Management Team. During this process, the Project Director will remain the primary point-of-contact for the FCO and owner of the escalation procedure. We will ascertain subcontractor partial or non-performance through quarterly reviews against KPIs. We will always try to resolve subcontractor issues informally first where possible, agreeing clear action points with timescales, escalating to Performance Improvement Process (PIP), Senior Management Team or independent dispute resolution as a last resort. From the outset of the contract, we will highlight the interests and needs of the ultimate beneficiaries – the Network Members – to ensure they are at the forefront of the subcontractor's approach. In this way, we have a constructive basis on which to discuss subcontractor performance.

Where informal resolution is not possible and performance is below 80% of agreed KPI standard, we will implement performance improvement measures, such as seconding ZINC staff, providing best practice guidance, or instituting stricter sign-off of deliverables. The objective of this process is to support the subcontractor to improve performance to a satisfactory threshold. We will focus on a solution in the interests of our shared goal for successful project delivery, balancing the need to resolve the issue for the FCO with the need to maintain the stability and effectiveness of the supply chain. This support is provided on a daily, weekly or fortnightly basis, as required. Where under-performance persists, the subcontractor is removed and a suitable alternative is used. In order of priority this would be: a similar organisation; staff engaged by ZINC as consultants or delivery by ZINC core staff with relevant subject matter and language expertise. Sign-off from the FCO will always be obtained for any material changes to key staff or subcontractors.

1.7 Recommendations for Improvement

This project can be viewed as a test case for applying the Network Model to the challenge of disinformation further afield than just Europe. The Consortium proposes a broad range of activities within the framework of **BUILD – SUSTAIN - TRAIN - CAMPAIGN - SCALE**, alongside a monitoring and evaluation framework, which will enable the Project Board and the FCO to adapt the focus and tactics of the project in order to pursue maximum impact. Nevertheless, there are some additional aspects, other than those we have already noted outside of the Terms of Reference, in our five layered approach, that could also be useful specialisms and mechanisms to test the efficacy of different approaches, and ways in which the scope can be expanded to address a wider set of challenges.

These recommendations for improvement have been categorised into **EXPAND - FOCUS - ANALYSE**. Ideas outlined in EXPAND enable us to expand the network geographically, in the type and number of organisations included, and in its public prominence. Ideas outlined in FOCUS enable us to hone activity on key areas and to provide additional support in times of crisis. Ideas in ANALYSE will deepen research activities to provide a fuller picture of the extent of disinformation and effective responses to it.

EXPAND

Expansion of Network Members

The current parameters of the project largely focus on Civil Society Organisations (CSOs). Adding different member groups to the Network, consisting of high-level practitioners in the field and formalising activity in the Scale strand, could further enhance the credibility of the network, increase support for this area of work and provide further opportunity to deliver impact against KPIs.

These groups could include:

- Leaders from the journalism and social media sector
- Leading think tanks
- Government partners

Geographical Expansion

The current proposal offers a categorisation of CSOs in three tiers based on geographic context and impact. This system could be built upon to offer additional tiers outside of the current geographic area, with different offerings for each tier. Outside of the current geographic scope, the Network could include MENA, Syria and the Levant, Central Asia or South America, reflecting emerging FCO priorities and the rise of disinformation in each context. This would enable the FCO to move quickly and flexibly, increase coordination across the FCO and overseas network, and would provide value for money as expansion would be enabled by using the existing footprint. Our current partners around the world would enable quick mobilisation into new regions, and could respond quickly to crises in order to measure and learn from events as they happen in the local context. As an example, our work could move to the Levant, building on the work that we have already undertaken through DFRLab and with May Day to scrutinise the disinformation around chemical attacks and the White Helmets in Syria.

Enhancing Credibility

To be sustainable and less vulnerable to attack from malign actors, the Network needs to be public-facing with a clear communications strategy that covers objectives and activities of the Network. This is discussed in more detail in 1.9. However, within the current scope of work, the strategy for public facing communications is based on minimum requirements, such as a static website, rather than proactive communications about or from the network as a whole. The project could expand to build on this public facing component, promoting the network as a journalist integrity and disinformation network bringing together all the actors in the field and further promoting their outputs.

FOCUS

Elections Focus

Elections are often a flashpoint for disinformation and foreign interference. Alongside existing activity, the Network could focus project resource on elections taking place in countries that are of particular interest to the FCO. The Network would bring together the expertise from the Consortium partners and the technical assistance pool to monitor the online communications around the election three months ahead of the event, identifying key trends and flashpoints in activity or narratives. This activity could be intensified six weeks prior to the election itself, accompanied with the training of Network Members operating in the country to expose disinformation and promote election integrity. The team could test different approaches to engage targeted audiences through mainstream media or governments, providing lessons learned and case studies that would feed into peer to peer learning. We could also work with social media providers and feed our findings into our SCALE strand with multilateral institutions and governments. We could also build some Network Members into a longer-term election cluster of organisations who prioritise this in their routine activity, building learning offers around this.

Rapid Response Vehicle

Our proposal already integrates a rapid response mechanism, facilitating a crisis response team comprised of technical experts with legal, security and communications expertise to support organisations at critical moments. However, this could be expanded to be a larger venture with more days allocated, able to respond to a larger number of organisations.

ANALYSE

Research

An expanded research component could generate better understanding of the drivers (psychological, socio-political, cultural and environmental) of those who are susceptible to disinformation. This will allow us to map vulnerable audiences, and build scenario planning models to test the efficiency of different activities to build resilience of those populations over time. Either through the re-analysis of datasets and insights from complementary FCO disinformation projects, or new quantitative and qualitative research, psychographic segmentation will assess what different attitudinal groupings exist, and what kinds of messages are important to them. Cluster analysis will group individuals by attitudes, overlaid with traits (e.g. demographics, lifestyles, media consumption, cultural context), to create "personas". These will be enhanced with behavioural insights gathered from qualitative research and/or linguistic analysis of online conversations to provide a 360 picture of:

- The individual context - Who the person is: values, attitudes, beliefs; self and social identity
- The cultural context – Who's around them, what do they hear: community, influencers, social norms
- The environmental context – What do they experience around them, where are they in life: politics, economics, geography, media, comms/messaging, education/knowledge

Understanding audience segments in this way will sharpen messaging frameworks, helping CSO partners to make the most of cognitive biases to target specific audiences, get maximum cut-through and resonance, and build stronger resilience to disinformation.

Building Resilience through Collective Journalism

Critical thinking and evidence-based reasoning are essential for countering disinformation. While the Terms of Reference focuses on organisations, we recommend expanding the scope to look at how to include the wider population, including small groups that may not be official organisations, individual activists, and concerned citizens in a model similar to that employed by the Latvian Elves. This would connect organisations with a larger pool of volunteers and capitalise on the small amounts of time that individuals can offer. This could look like the creation of a neutral, fact-checking and disinformation de-bunking hub available in multiple languages.

Rather than just passively consuming messages, if we actively engage people in collective fact checking and reasoned arguments, we will help them confirm or invalidate statements, explain the evaluation clearly and build up their resilience to disinformation. Allowing groups of people to work through this process together, with each person handling small pieces that can be assembled into a complete evaluation of a statement or claim, will speed up the fact-checking and counter-disinformation process. Via an online hub - in multiple languages (potentially a unique resource) - people will create new enquiries or engage in ongoing ones. This will allow groups of people to work through a complete evaluation together, each handling the amount of information they feel comfortable working with.

To fact-check a statement, for example, a user (an engaged citizen or CSO partner) might post an assertion made in the news or on social media. Other users could then contribute related stances, claims, evidence and sources. Each addition helps flesh out the formal argument structure with additional information. Having a neutral, ad-free news and information platform available in multiple languages would be a unique opportunity for the FCO to amplify and harness the power of the voices that audiences trust most: people like themselves.

Open Source Research

The ever-shifting nature of disinformation needs agile responses. Our CSO partners are likely to be forced to shift rapidly from one topic to the next. Whilst we will be generating a wealth of data and insight from this project, there is unlikely to be time and capacity to analyse and understand all of it from all angles and in-depth.

Open-source research, whereby we publish anonymised datasets and project updates on a centralised hub, in usable, editable formats, will allow the research community to collaborate easily on the project. They will help fill gaps and create links that allow analysts to better understand fragmented narratives, rumoured motives, possible sources and potential real-world impacts. This will strengthen thinking and help evolve strategies, processes and impact evaluation.

1.8 Sustainability

The approach has been designed with sustainability at its core. Each pillar of our operating model (described in section 1.5) is designed to ensure long-term technical and financial sustainability of project beneficiaries in different ways. We will *build* a network to address organisations' isolation and lack of coordination, we will *sustain* them through upskilling in long-term financial planning and reducing cyber and legal risk, we will *train* them in order to increase their technical ability in exposing disinformation and support them with *campaign* skills to communicate to broader audiences. Uniquely, our approach also includes a *scale* strand, with a focus on increasing the sustainability of the sector as a whole through ensuring that shared protocols and standards are understood amongst policy makers, governments, tech companies and grassroots implementors. This will reduce the risk inherent in investing in the sector, further cross-sector collaboration, and build the market for countering disinformation. Our approach to sustainability targets three layers; sustainability at the level of the **individual organisation**, the level of **partnerships** and cluster building, and also the **sector as a whole**.

Increasing the Long-term Sustainability of Individual Beneficiaries

Organisations are vulnerable at four key points; their financial sustainability, their technical skill sets, and their legal and security risks. Crucially, all the support provided at each of these four points will be provided in a tapered fashion to ensure long-term equipping over the three-year period, integrated with their current team, size and activities rather than a sudden short burst of activity.

Technical Skill Enhancement

Our Consortium, outlined in section 1.5, believes that learning is best achieved in a collaborative environment with civil society organisations (CSOs) acting as equal partners in order to achieve clear buy-in to the mutually agreed objectives. Our Network Managers will be responsible for ongoing needs assessments and setting learning goals for each organisation united by the following characteristics:

- **Collaborative and locally owned and driven**. Each activity will be flexible with different options available depending on the specific need and context faced by each organisation. A bottom-up model will be developed where Network Members share their needs with Network Managers, adapting learning plans accordingly. Results frameworks will similarly be designed and owned by each organisation with support from the M&E team.
- **Focused on co-creation and embedded learning.** Although traditional training sessions will feature in the offer, there will be a focus on co-creation of outputs such as research and communications products, and on embedded learning where experts will sit with organisations over an extended period of time to upskill them.
- **Addressing knowledge, skills and attitudes.** Learning will ensure that technical skills are accompanied with a focus on increasing motivation and confidence in exposing Russian state backed disinformation.

Reducing Legal and Security Risks

Organisations are at risk from hostile actions which could include litigation or cyber-attack. These actions will ultimately reduce their ability to continue to deliver this work over the long-term, and reducing these risks must therefore be a key feature of the project. We will focus on:

- **Reducing libel risk**, training on how to avoid engaging in practices that could provoke libel complaints, and reviewing key pieces of content drawing on our pool of experts including James Wilson.
- **Setting up adequate insurance and support provision.** We have dedicated budget for professional indemnity insurance, which organisations themselves will take out, and we will also encourage organisations to find legal pro-support locally and broker connections when necessary.
- **Providing basic legal training.** Organisations will receive training in GDPR, how to protect themselves against corruption risks and other elements in order to ensure they are operating within all applicable legal frameworks and ethical guidelines.
- **Upskilling in crisis communications.** In the event of an attack, organisations will need to rapidly respond with precision and in a way that limits their reputational risk. We will train them in skills including crisis communications, safeguarding team members, designing emergency protocols, and will provide a rapid response support service.
- **Cyber security.** We will deliver training and support, including a secure communications portal for project communications, reducing the risk of attack.

CASE STUDY: Increasing the sustainability of Tunisian activists. In 2017 ZINC ran a training programme for 16 youth social activists in Tunisia supporting them to reach wider audiences and professionalise their digital communications. Participants had no previous training in legal best practice or media law and faced risks that risked their sustainability. A component of this training therefore taught them legal best practices including: sourcing content from archives, consent and non-disclosure, and permission for filming in public. These activists went on to develop 35 pieces of content adhering to legal best practice, and set up processes for future work.

Financial Sustainability

To improve the financial sustainability of Network Members under our *Sustain* strand our Network Managers will develop a bespoke business growth strategy for each organisation. This strategy will look at how to develop their business models to attract different types of funding and assess their commercial viability.

- **Business planning** – a three-year business growth strategy for each organisation will be developed, alongside training and mentoring addressing how to develop a business model. Our consortium will utilise the lessons learned from the experience of supporting scalable independent media in the Baltic States in 2017 with an emphasis on building financial sustainability through robust business planning, fundraising and cooperation with local investors. Network Managers will work with each organisation to look at how to diversify funding streams and improve commercial viability.
- **Grant proposal training** – organisations will be trained on how to write successful grant applications and design budgets, and members will be supported through the application process.
- **Core funding** – funding will be delivered to a minimum of 20 organisations, managed through the small grants programme, which will be designed to build the organisation. A core criteria of award allocation will be how activities point to long term sustainability – e.g. through employing a fundraising manager.
- We will also facilitate **new funding partnerships** between Network Members and potential donor organisations and/or private investors, setting them up for future support and opportunity to maintain independence and sustainability of the CSOs through a diversified source of funds.

Strengthening partnerships to reduce isolation

A key tactic of the Kremlin is to isolate organisations, leaving their reputation questioned, and increasing their vulnerability. It is therefore vital that the project invests in both building partnerships and strengthening partnerships that already exist. To encourage partnerships the Network will:

- **Build regional and thematic clusters** and smaller groups of organisations working on cross-cutting issues, where organisations will be encouraged to share knowledge, learnings and skills.
- **Link clusters with experts.** They will be supported to invest in a community and to work together through synergies, linked with experts from fields including cyber security and safeguarding, and encouraged to discuss and mitigate against hostile attacks.
- **Facilitate peer to peer learning**. Learning between Network Members will also play a pivotal role in sustainability ensuring that learning is mutual and locally embedded, rather than top-down. This learning process will facilitate new solutions and approaches leading to a self-sustaining network more capable to tackle malign influence with less, if any, external assistance.
- **Promote the network to other donors**. Opportunities will be actively sought to obtain new sources of funding (for discrete activities, clusters, or individual organisations) from external agencies, such as HQ NATO, US Foundations, and private companies committed to counter disinformation i.e. Facebook, Twitter, etc. The Consortium works closely with the US Government and the EU and will broker these partnerships to build the reputation of the network and its clusters and members among potential funding sources. This will be carried out under the guidance and auspices of the FCO.

Driving the long-term sustainability of the sector

Alongside enhancing the sustainability of individual Network Members and focusing on strengthening partnerships and clusters of organisations, this proposal also aims to invest into the sector as a whole. **This is an added value not referenced in the ToR, and a strand that we believe critical to the project's long-term success.** A vigorous, visible, well-funded sector researching and countering disinformation through a variety of tested tactics is the only way to ensure the sustainability of these individual organisations after the initial three-year network project. This will be achieved through:

- **Bringing together all the key actors invested in countering disinformation**, currently implementing disparate activities and operating in siloes, including tech companies, international media outlets, governments and policymakers. The Digital Forensic Research Lab (DFRLab), referenced in section 1.5, will lead a strand of work that convenes discussion and debate, bringing these actors together around shared vision and outcomes.

- **Using learning opportunities to promote growth.** The Hub will build on the successes of Network Members in exposing disinformation by encouraging other organisations to test similar strategies. Replication of impact and growth will be the driving force behind the network, with success leading to increased investment in the sector.
- **Injecting professionalism through setting standards and protocols**. Utilising the expertise of organisations, including Bellingcat and DFRLab, presents a unique opportunity to invest in setting standards and protocols for specific activities, e.g. how to attribute accounts or activity with a low margin for error. If work adheres to common sets of standards, then the risk reduces for those delivering the work and for those funding it. This will lead to greater prospects for long-term investment in the sector.
- **Raising awareness of the threat faced**. Through upskilling organisations to expose the actions of the Kremlin to deceive and mislead, and conducting activities including roundtables and policy dissemination, a greater proportion of academics, governments and the mainstream media will understand its pervasiveness and the complexity and gravity of the threat. This will drive research, understanding, and help to raise the profile of the important work done by organisations in this sector, ultimately increasing its sustainability.

1.9 Operating Environment

Network Model and Strategic Approach

The Network strategy we propose responds to (1) the scale and geographical spread of the Network, (2) the unpredictability of geopolitical events and the support Network Members will require, and (3) the highly locally-specific tactics of the Kremlin disinformation network. It does so by using a team of regionally-embedded and expert Network Managers to act as a conduit between the centre and periphery, driving forward the overall project strategy and commissioning the specific support from the centre that members in their region need to operate effectively. This will promote:

- **Trust** between members and the project
- **Local** development of solutions and
- **Flexibility** to respond to events and adapt the project's work to changing circumstances.

Our Network Managers have been specifically chosen for their geopolitical knowledge and expertise within their region, and their experience of media development and/or disinformation. An acute understanding of the challenges that Network Members face will give Network Managers the credibility they need to work effectively with members.

As well as facilitating the transmission of information and provision of support between the Hub and members, Network Managers will facilitate network effects between members. By encouraging cooperation within regional clusters and through ad hoc groups on specific issues, the approach will recognise that the supported organisations themselves are a key source of experience and best practice. Further, this approach will reduce the isolation that is a common feature of partner organisations' experience – and something frequently capitalised on by the Kremlin.

CASE STUDY: Building a Network in Ukraine. Our consortium has a proven track record of designing context-specific operating models that reflect local context, political dynamics and sensitivities in order to manage risks and avoid hostility and suspicion. In Ukraine, we worked with online influencers to equip them to counter Kremlin-backed messaging through innovative editorial strategies, audience segmentation, and production models that reflected the complex and sensitive political environment. As a result, the group of 12 were able to reach wider audiences with compelling content that received over 4 million views.

Selecting and On-boarding Network Members

The Consortium's wide reach ensures existing relationships with every organisation identified by the FCO, and the ability to immediately onboard selected organisations. Through the inception phase, the Advisory Panel and Project Director will work from the FCO's list of identified organisations to undertake further due diligence if necessary, risk identification and mitigation, and prioritization, and to allocate each network member to a tier. We will divide members into tiers **based on (1) the FCO's regional focus and (2) impact factor** (potential to influence target audiences):

- ***Tier One: High Impact, 12 Priority Countries*** *(30% of organisations) anticipated to be drawn from the Baltic States, Moldova, Georgia, Ukraine, Belarus the Visegrad Four, and the Western Balkans.*
- ***Tier Two: High Impact, Rest of Europe*** *(40% of organisations)*
- ***Tier Three: Lower Impact, 12 Priority Countries*** (30% of organisations).

Tiering will enable resources (including core support – delivered through grant funding, discussed further in section 1.5) to be focused most effectively. Tiers will be adjusted over time to reflect geopolitical changes, flexibility to follow emerging FCO priorities, new organisations being approached and onboarded and reacting to opportunities to deliver impact as they arise.

Making use of our existing contacts with the identified organisations, Network Members will then be supported to make contact and begin the process of onboarding members to the Network, making use of customisable materials on the purpose, benefits and operating model of the project, produced by the Hub to smooth and speed this roll-out across the regional clusters. The onboarding of new members not initially named in the ToR will require additional due diligence, which will be conducted with consideration for independence, integrity and the risk of Russian influence.

Working with Network Members

Each Network Manager will produce a comprehensive stakeholder map – focusing on members but also including non-members – setting out a stakeholder management schedule, include **minimum contact schedules** and appropriate lines of communication, helping them fulfill their role in understanding members' work and needs and connecting them to the project Hub. Network Managers broker a two-way relationship between members and the project:

1. The Advisory Panel, Project Board (see organogram for further detail) and Project Director identify opportunities and threats and set an overall strategy for the project. This is communicated through to Network Managers, who tailor regional tactics – using their knowledge of members' positioning and strengths – to deliver the strategy. This ensures the strategy is delivered through locally-relevant work that is more likely to have impact.
2. Network Managers will assess individual members, identify their needs and design and 'commission' bespoke packages of support for them from the project Hub and associated experts (including core support / grant funding where appropriate). This puts those with the most up-to-date and detailed knowledge of Members and the context they operate in at the centre of determining how the Network's resources are brought to bear in response to the complex and evolving challenge posed by the Kremlin's disinformation network.

Commitment and Ownership through Collaboration

Network Managers will have a role in clearly articulating the benefits of Network Membership to encourage participation and commitment. However, in our work with media organisations across Europe, we have found that trust - built up through transparency, regular contact and support based on collaboration and co-creation as opposed to didactic information dissemination – is key to generating high levels of commitment from partner organisations.

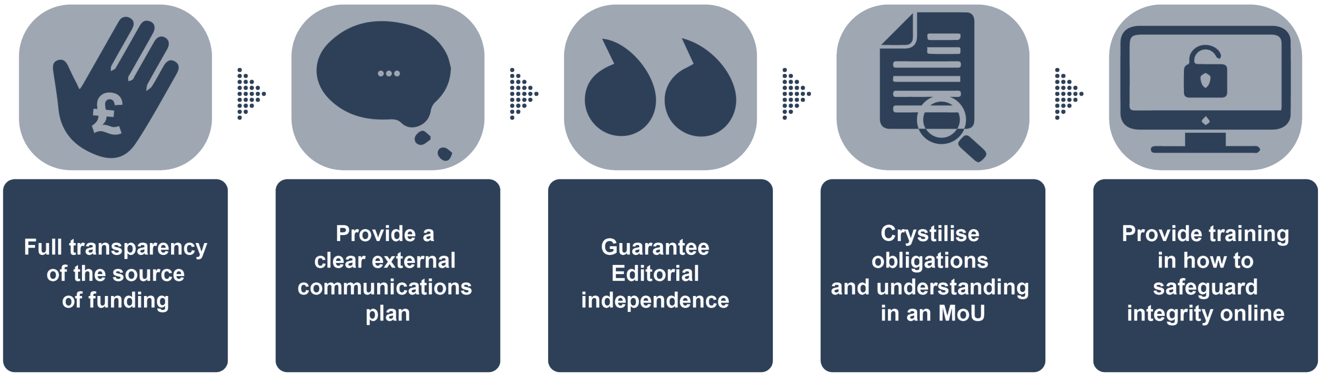
- **Sustain:** Civil Society Organisations **(**CSOs) will work with their Network Manager to build an **integrated sustainability plan**, pulling in resources from the short-term technical assistance pool. Support available will include: funding proposals, budgeting and business models, funding sources, M&E, and digital security including secure communications. Network Managers will identify context-appropriate opportunities to deliver this sustainability support – i.e. when it is most relevant to actual work members are carrying out, making it timely, relevant and useful. This demonstration of the project's commitment to members' long-term success will help build trust from the outset.
- **Train:** Network Managers will assess members' most urgent training needs and design a capacity building plan to address them so as to **maximise their impact in the context of the overall project strategy**. Tier One members will have access to embedded Bellingcat mentors who will work with them on a high-impact research or investigative journalism project, end-to-end, deepening the relationship. The project will also support members on maximising the effectiveness of their digital output. Finally, Network Managers will identify any need for more one-to-one support, including libel review of output and crisis communications. Capacity building that takes place by working *alongside* members has the best chance of promoting trust, commitment and ownership.
- **Campaign:** As well as upskilling members on campaign strategy, a key plank of support will be **campaign co-creation**. This approach – pioneered by the consortium in previous projects – will be a key way that the overall project strategy is delivered. It also ensures that campaigning support is anchored in real – not theoretical – issues that members care deeply about and want urgently to campaign on.

Our approach to delivering the project strategy and supporting and building the capacity of members treats them as **equal partners who co-develop solutions to the disinformation crisis**. It recognises their knowledge of the local context, the regional experts, and the disinformation narratives that have gained traction and stuck. Our support is built around their wants, our assessment of their needs, and the project's strategic aims. The Consortium also has the structures and processes to enable tailoring to these needs and the operating environment, enabling a quick and dynamic response in situations of crisis.

CASE STUDY: Locally owned insights in Ukraine, Moldova and Belarus. In 2018, the Consortium delivered audience insights and recommendations to increase reach and resonance of selected independent media outlets in Ukraine, Moldova and Belarus. The project design was co-developed with local beneficiaries and utilised a partnership model which the EXPOSE Network can build on. This partnership model ensured research outputs were co-owned and developed iteratively. As a result of this local ownership the insights were successfully integrated into the outlet's strategic planning and actions to take in 2018-2019, resulting in an increased audience share across the board.

Editorial Independence

Full editorial independence is vital for members' credibility (and therefore effectiveness) and to manage risks to the FCO in project implementation. Members will remain fully in control of, and responsible for, their output and must operate on the basis of internationally recognised standards of journalistic ethics and editorial integrity. Beneficiaries and Network Managers will undertake specific training, delivered by Media Diversity Institute (MDI), on journalism ethics. Our experience supporting independent media in the Baltic States and Eastern Europe has highlighted five key rules that assist in ensuring functional editorial independence, which will be designed into this project. These are detailed below.


Full transparency of the source of funding
Provide a clear external communications plan
Guarantee Editorial independence
Crystilise obligations and understanding in an MoU
Provide training in how to safeguard integrity online

Code of Conduct

We will establish a Code of Conduct for Network Members, and a framework of protocols aimed at delivering operational safety and increasing buy-in. This will include (but not be limited to): storage of information and data, logging of lessons learned, information and intelligence sharing on malicious actor activity, network communications and information transfer. We also propose a **minimum required engagement** caveat for Network Members. These expectations – as well as what members can expect from the project - will be managed by Network Managers.

Non-Member Stakeholders

Network Managers are responsible for the project's interface with non-member stakeholders in their regional clusters, including local British Embassies under the direction of EECAD. Key stakeholders include:

- Governmental agencies
- The media

Governmental

The Consortium's experience working with the FCO, international governments, donors and the media will inform the tools and processes used by Network Managers to coordinate with governmental stakeholders. During inception, each Network Manager will develop, for each country in their cluster, a matrix covering:

- Governmental stakeholders;
- Milestones in the project cycle where we envisage greater stakeholder engagement: in particular during project inception and events of geopolitical significance
- Key individual contacts;
- Stakeholders' preferred channels and methods for information exchange.

These matrixes serve as a Network Manager's tool for (i) staying abreast of risks and opportunities relevant to the project – in particular any potential for work to feed into partner government efforts (see 1.7) – and (ii) keeping stakeholders informed, bought into and supportive of the project, smoothing the operating environment. Network Managers will also work with locally-active donors (USA, EU etc.) to understand their strategic priorities and current portfolios, identifying potential areas for collaboration and/or co-funding, with support in identifying opportunities from the Advisory Panel.

CASE STUDY: Complex cross-government stakeholder management in Tunisia. In Tunis, the Consortium's counter-terrorist work had a robust stakeholder management mechanism with local government agencies and the British Embassy based on weekly reporting and monthly meetings that ensured greater local commitment and ownership of the project results. Multiple government stakeholders (including the FCO, RICU and different ministries within the Tunisian Government) were closely involved in activities, brought together around shared objectives with clear points for communication and feedback.

Media

Key media relationships will remain at the member level. Network Managers will ensure project support to members amplifies their ability to build and nurture media relationships. Beyond this Network Managers will use their own networks and profile to act as advocates of the project, ensuring visibility of members and facilitating introductions. In particular, Network Managers will focus on building up a go-to list of talking heads for journalists in their regional cluster to draw upon as needed.

Where specific opportunities are identified by the Advisory Panel or members, exclusive media partnerships may be negotiated. These relationships would ensure that content from CSOs is regularly featured in key media outlets in country; increasing visibility and reach of content and reaching audiences. This would also add further sustainability to the CSOs reach once the project reaches its conclusion.

Expanding the Network

Our consortium is uniquely well-positioned to expand the Network by identifying and working with organisations beyond those already selected by the FCO. Gaining access to additional geographies, sectors and tactics by adding to the Network is a key way the Consortium will add value, going beyond the ToR. Across Europe and beyond we have pioneered network-building as a strategic approach to disinformation and communications challenges.

We expect Network Members will lead us to new organisations. Alongside this, Network Managers will actively source potential new partners through a well-established, international, English-language network of peer specialists dealing with Russian disinformation and related issues to which we have access. The breadth of sector expertise represented in the Consortium ensures we are uniquely placed to identify a wide range of organisations, including those not necessarily self-aligning with the countering disinformation sector. This includes:

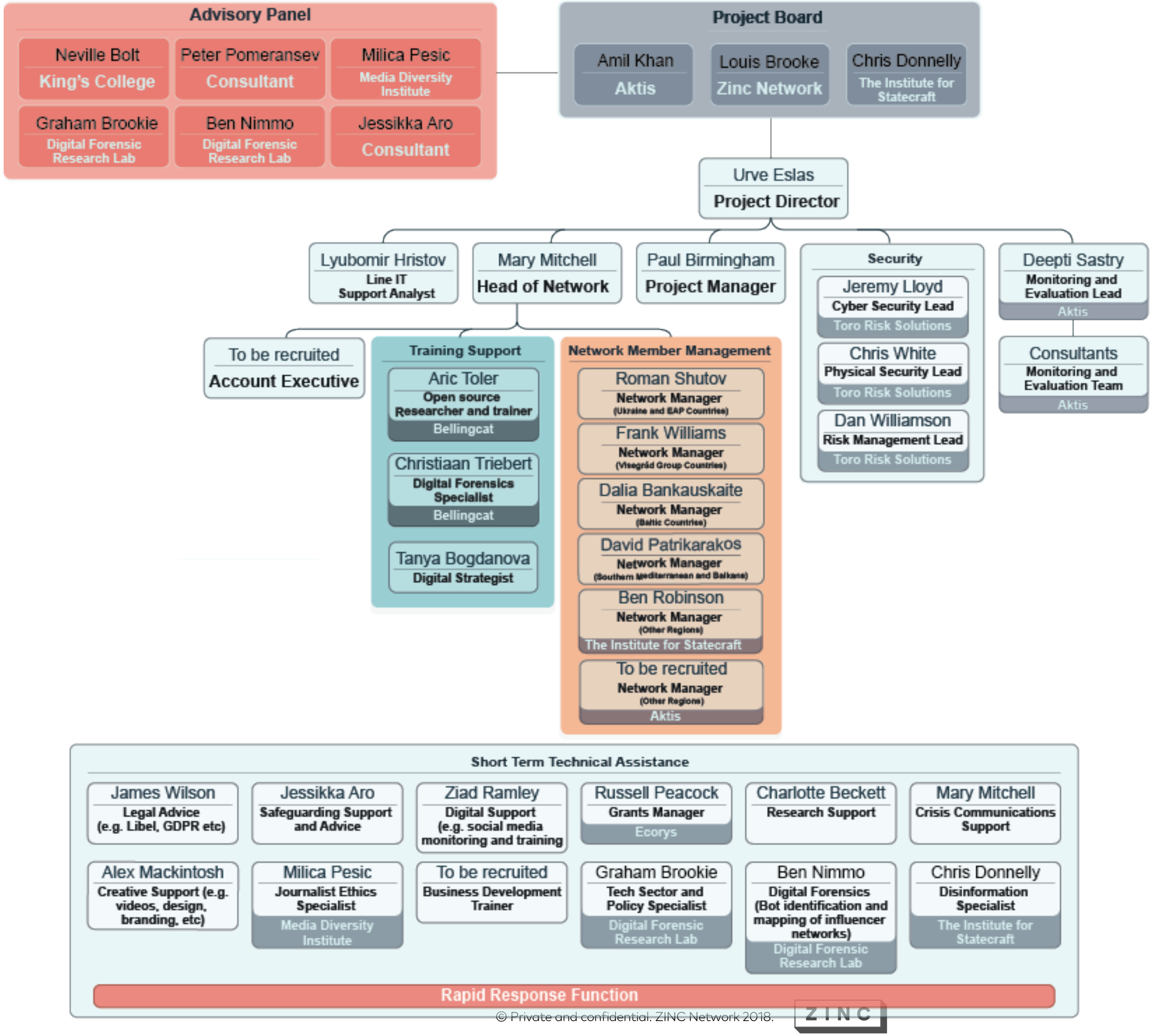
- MDI's long-standing work and reputation with media outlets across Europe ensures they can identify emerging journalism and media partners
- DFRLab's policy outputs and expertise tracking and monitoring disinformation leads them to identify research organisations with potential in this space
- The Institute for Statecraft's Integrity Initiative provides a pre-existing pool of contacts as a springboard for the identification of new potential Network Members
- ZINC's work with online influencers and new media creators will lead us to those best placed to deliver public-facing campaigns.

Vetting and Selection

In line with our prior due diligence on the FCO's identified list of organisations, we will vet any potential new members according to the due diligence set-out in our *Build* stage with Toro, our security partner. The contacts we will use to identify potential new partners have detailed knowledge of the strengths, weaknesses, internal disputes and finances of the CSOs in question. This will ensure another layer of due diligence which will be set against the geographical alignment and impact factor of any potential new member for selection.

THE MEDIA INTEGRITY NETWORK: Positioning the Network for engagement with wider stakeholders
The public-facing brand and positioning of the network is essential to successful stakeholder management, particularly government partners and the media. We propose establishing a brand identity and clear mission statement that positions the network squarely in the media integrity space, referencing the range of supporting organisations. Communication about specific activities will be minimal, but this will serve as a focal point for discussions and will reduce suspicion about the network. When linked to a broader, coherent entity, organisations themselves will be less isolated and susceptible to risk. Managing this brand and the communications strategy within the context of a wider risk management framework will be a crucial task for the Project Director and wider team.

1.10 Resource Project Team Organogram



Advisory Panel

- Neville Bolt, King's College
- Peter Pomeransev, Consultant
- Milica Pesic, Media Diversity Institute
- Graham Brookie, Digital Forensic Research Lab
- Ben Nimmo, Digital Forensic Research Lab
- Jessikka Aro, Consultant

Project Board

- Amil Khan, Aktis
- Louis Brooke, Zinc Network
- Chris Donnelly, The Institute for Statecraft

Urve Eslas, Project Director

- Lyubomir Hristov, Line IT Support Analyst
- Mary Mitchell, Head of Network
- Paul Birmingham, Project Manager
- Deepti Sastry, Monitoring and Evaluation Lead, Aktis
- Consultants, Monitoring and Evaluation Team, Aktis

Security

- Jeremy Lloyd, Cyber Security Lead, Toro Risk Solutions
- Chris White, Physical Security Lead, Toro Risk Solutions
- Dan Williamson, Risk Management Lead, Toro Risk Solutions

To be recruited, Account Executive

Training Support

- Aric Toler, Open source Researcher and trainer, Bellingcat
- Christiaan Triebert, Digital Forensics Specialist, Bellingcat
- Tanya Bogdanova, Digital Strategist

Network Member Management

- Roman Shutov, Network Manager (Ukraine and EAP Countries)
- Frank Williams, Network Manager (Visegrád Group Countries)
- Dalia Bankauskaite, Network Manager (Baltic Countries)
- David Patrikarakos, Network Manager (Southern Mediterranean and Balkans)
- Ben Robinson, Network Manager (Other Regions), The Institute for Statecraft
- To be recruited, Network Manager (Other Regions), Aktis

Short Term Technical Assistance

- James Wilson, Legal Advice (e.g. Libel, GDPR etc)
- Jessikka Aro, Safeguarding Support and Advice
- Ziad Ramley, Digital Support (e.g. social media monitoring and training
- Russell Peacock, Grants Manager, Ecorys
- Charlotte Beckett, Research Support
- Mary Mitchell, Crisis Communications Support
- Alex Mackintosh, Creative Support (e.g. videos, design, branding, etc)
- Milica Pesic, Journalist Ethics Specialist, Media Diversity Institute
- To be recruited, Business Development Trainer
- Graham Brookie, Tech Sector and Policy Specialist, Digital Forensic Research Lab
- Ben Nimmo, Digital Forensics (Bot identification and mapping of influencer networks), Digital Forensic Research Lab
- Chris Donnelly, Disinformation Specialist, The Institute for Statecraft

Rapid Response Function

1.11 Risk Management

Risk Environment and Approach

Risk is an unavoidable aspect of this project. The work is antagonistic by its very nature (viz-a-viz an actor proven to act against those who threaten its interests). It is a highly complex project involving coordination of many independent actors; and, given the project's public profile and the broader context, it is likely to attract significant media attention. This means that unmanaged risks could undermine not only the project's effectiveness but also the FCO's broader reputation, credibility and relationships in this space. However, although these serious risks must be robustly managed, they cannot be *managed out.* Network Members are - almost by definition - risk-takers, and the project will fail if it inculcates risk-averseness in members. Rather, it must ***identify***, ***monitor and manage*** risks as they materialise, allowing members to continue taking smart risks as they increase the scale and impact of their activities. Neither the project nor the client can absorb or take liability for risks taken by Network Members. For the project to be effective and viable, members must maintain both organisational and editorial independence. The project's role will be to **support Network Managers and members** to plan for and better-manage risks themselves and increase their resilience when risks do materialise.

Understanding Risk

We group project level risks into three categories; **operational** (legal, financial, cyber, physical), **delivery** (threats to the effectiveness of project delivery) and **reputational**, set out in the indicative risk register below. Members - as part of the ecosystem the Kremlin seeks to undermine - also face a number of risks: direct on-/offline attacks, disinformation, and being bogged down or bankrupted by vexatious litigation. These risks are by extension a risk to the project and client therefore we have placed **safeguarding** (discussed in depth in 1.2 and 1.3) at the centre of the project's approach and procedures, to build members' understanding of, ability to manage, and resilience to risk.

Identifying and Monitoring Risk

Risk is best identified and monitored by those exposed to it. The project aims to build the capacity of members to identify and monitor risk and to aggregate that insight at the project level to enable action to manage that risk as required. Led by our risk management partner Toro, we will risk assess each member across both physical and cyber security. For the 10 Members deemed to be highest risk, this will include a comprehensive site visit to assess their physical and cyber security requirements. Drawing on Toro's expertise, these assessments will be used to build a risk management framework to cover risks to members. Each member will be trained and supported to develop and maintain a risk register, covering the risk categories outlined above. These will feed into the project-level risk register, owned by the Project Director, which will be reviewed and reported on weekly, and comprehensively reviewed with the support of independent risk and security advisors monthly; prior to contract management meetings. This will serve as an overarching risk register and risk management system, collating risk from the individual partners and the consortium partners, giving a sense of the overall risk level across the portfolio, identifying cross-cutting risks, and enabling a more precise response.

Managing Risks

Risk management and mitigation have been addressed at a number of levels, including:
Project and organisational design: (1) ensuring the editorial integrity and independence of all members (through journalist ethics training and oversight by MDI and content review by Network Managers), (2) a clear public brand for the project which positions it as part of a broader effort to support integrity in media in line with internationally accepted standards and (3) embedding accountability and responsibility for safeguarding throughout the organisational structure.
In-kind specialist support to help members to help manage risks including: 278 days of legal and compliance support for members with Legal Advice from James Wilson and his team, reviewing key outputs for libel and other litigation risks and reviewing project and member activities to ensure they are fully compliant with relevant regulations including GDPR; 300 days of physical and cyber security support; 100 days for crisis response and critical incident response support across the project drawn from all staff.
Risk management training: to ensure members have the tools to plan and respond when threats do materialise and will do so sustainably. Recognising that members have evolved their own tactics to dealing with attacks, we'll leverage their experience to develop **a playbook of best practice** that can be shared across the Network, reducing the isolation that the Kremlin seeks to takes advantage of. Each member will receive a training course

on cyber security and support to implement basic resilience and response factors as well as two day training on risk management including physical security, critical incident response and be supported to establish appropriate policies and procedures. Separately, members will receive training on libel and data protection regulations.

Ongoing Management: Network Managers – with the best information on individual members, their capabilities and risk tolerance – will ensure **activities are calibrated so as to avoid exposing Members to inappropriate levels of risk**. They'll see that risks are managed at member level and are escalated through to the Project Director and Advisory Panel where appropriate. In particular, serious and urgent safeguarding risks – identified during planning – will be subject to an accelerated escalation mechanism to manage serious risks of physical harm or irreversible property or systems damage. Ongoing training and on-demand support from the risk and security advisor will help members and Network Managers to respond to risks as they materialise.

Building organisational resilience of Network Managers to risks that materialise: Ensuring, and where necessary providing financial and administrative support for them to procure professional indemnity insurance and securing local *pro bono* legal and cyber support from leading firms and providers in their region. This will also include providing cyber support to ensure deterrence, access to a content reviewer to mitigate against libel accusations, a fund for public liability insurance for up to 20 high-risk organisations to ensure they have resources to respond to vexatious litigation, a cyber reporting function to monitor the network for attacks, and personal safeguarding training.

Collaboration across the Network: will be vital in allowing Members to support each other in managing risks. The Account Director will promote the formation of **ad hoc committees** of Members on specific risks, for example those faced by women, in recognition of the fact that women working in this space tend to face a higher risk due to the Kremlin leveraging the unequal standards expected of women in public life in an effort to shame and constrain them.

CRITICAL INCIDENT RESPONSE: Responding rapidly to crisis and managing risk
Network Members will be faced with the possibility of hostile external activity on many fronts including the threat of litigation and cyber or physical attacks. Organisations need to be confident to continue their work exposing the Kremlin's malign information activities while knowing that there is a framework in place to protect them. In addition to the ongoing activities outlined above, we will operate a rapid response function, deploying a team of specialists to support in the event of crisis. This team of specialists will support the organisation with crisis communications, and security and legal advice.

CASE STUDY: Risk management and rapid response. Our established Staff Safety and Risk Management policy details our approach to Duty of Care and the oversight, management and implementation of operational risk / security management protocols and procedures. This policy has minimised incidents over the years, and the few emergency situations we have had have been successfully managed through a robust Crisis Management Plan. In 2016 during delivery of the Suuqa contract in Somalia, Al-Shabab carried out a bomb attack on Mogadishu's Lido beach restaurant. One national staff member was seriously wounded. Our Risk Manager travelled to Somalia to manage the incident locally. Local knowledge and contacts ensured the staff member could be moved to the best available private medical facility within 60 minutes of injury. Insurer arranged MEDEVAC for best available medical care in Kenya and senior staff deployed for post-incident follow-up.

Below is an illustrative risk register, which will be written in detail and provided to the FCO for discussion at project inception.

Risk	Impact	Likelihood	Mitigation
Project Operational and Effectiveness			
Contracting, legal and financial management risks	High	Low	• Project Director's regular work with Advisory Committee • ZINC's project management and administration backstopping
Disruption to project continuity due to loss of sites or staff	High	Low	Overlapping key team skills and project continuity plan
Members' contribution falls short of expectations	Medium	Medium	Maintain flexibility to off- and on-board Members as required
Physical risk to project staff/sites or events	High	Low	Risk assessment, action plans and crisis management by RSA
Reputational			
Project interpreted as UK-sponsored disinformation or 'troll factory', seriously undermining UK reputation and agenda in this space	High	Medium	• Position the project in- and externally as being within the established and accepted sector of media development and pluralism and fact checking • Be explicit that Members are independent and bake this into operating model • Ensure Members operate with integrity and ethically
Interception and publication of project communications	High	Low	• Risk assessment, action plans and crisis management by RSA • Industry standard high-security communications and other tools
Member activity does not meet journalistic or ethical standards, undermining their credibility and bringing the project into disrepute			• Close monitoring of Member activities by Network Managers • Training by MDI on journalism and ethics alongside a Members code of conduct • Vetting of Members
Member Safeguarding			
Members exposed to higher profile/scrutiny/level of interference than they can handle	High	Medium	• Calibration of activities to Members' capabilities and risk tolerance • Escalation of high-risk issues to Project Director and Advisory Committee

Hacking of Member or project servers and/or communications that (i) disrupts their work, or (ii) reveals compromising information on Member organisations or individuals, or the project	High	Medium	• Risk assessment/cyber audit of all Members • Training on cyber-security and action plans to address weak spots • Industry standard high-security communications and other tools • Identification and escalation of serious threats by Network Managers • Critical incident management by project team as supported by RSA
Infiltration by force or subterfuge into Member organisations that either (i) disrupts their work or (ii) reveals sensitive information damaging Member or project credibility	High	Low	• Risk assessment of all Members and sites including visits to high risk sites • Training on physical security for Members • Identification and escalation of serious threats by Network Managers • Critical incident management by project team as supported by RSA
Vexatious and other litigation (in particular libel-based) constraining Members' freedom to act, delaying work or draining Members' financial resources	Medium	Medium	• Identification of high-risk jurisdictions • Legal training to Members • Legal review where necessary by expert libel consultant • Maintenance of liability insurance
Harassment, trolling, and doxing of individuals involved with Members	High	Medium	• Development of playbook of responses based on Members' experience • Collaboration among Members including through ad hoc committees • Emotional/other support • Crisis management by project team for serious incidents
Undermining of Member organisations through disinformation, distracting them or reducing their credibility	Low/Medium	High	• Development of playbook of responses based on Members' experience • Collaboration among Members including through ad hoc committees

1.12 Quality Monitoring

Our Approach

The very nature of disinformation, its multiple narratives and far-reaching ecosystems, means that this programme is taking place in a constantly-evolving risk environment and media landscape. This Network model will also be the first of its kind. An essential part of the programme, therefore, will be making the most of the data it's producing to understand impact, improve performance and ensure that the Network is empowered to work effectively. In doing so, the Network Managers and central M&E team is well placed to take a longitudinal and holistic view of the wider programme, and through close collaboration with the involved civil society organisations (CSOs), collect data for specific activities, campaigns and regions. We will collaborate with those CSOs to build the Network's monitoring and evaluation capacity and ensure that lessons learned are used to improve programme quality, creating an agile Network that creates real value through real-time, make-measure-learn feedback loops. Our Project Director will keep abreast of all deliverables, including any underperformance across all activities. In this instance, ZINC's well-defined poor performance procedures would be activated.

Continuously Monitoring and Improving the Quality of Network Services Delivered

We propose a mixed method approach, combining quantitative and qualitative techniques, allowing us to:

- empower the Network to use real-time data to iterate and respond to changes in context
- utilise longitudinal data to understand changes in behaviours resulting from capacity building activities and, consequently, iterate the nature/focus of activities
- use data to quantify and help sustain the impact of the programme over time
- evolve evaluation models over time to maximise service quality

These rich datasets will mean we will be able measure progress against our Theory of Change.

If a network of CSOs monitoring and exposing disinformation are brought together, facilitated by expert Network Managers, and equipped to upscale their activities:

Then

- Network members will have increased capacity to deliver effective counter-disinformation activities
- Activities will be anchored in research and data, audience insight and behavioural vulnerabilities will be revealed, and insight into disinformation strategies and tactics will be better understood
- Peer to peer knowledge sharing will be enhanced; successes and synergies shared, and gaps identified

Thereby

- Increasing the quality, quantity and impact of counter-disinformation content and strategies to tackle it
- Increasing the sustainability and professionalism of organisations countering disinformation
- Creating an ecosystem of credible voices which can continue to grow and counter the disinformation ecosystems exploited by Russian actors, reaching new and vulnerable audiences
- Helping to establish best practice on countering disinformation

Contributing to

- Increased awareness of Kremlin disinformation among expert and non-expert audiences
- Undermining the credibility, effectiveness and reach of Kremlin disinformation campaigns, and reducing or slowing down their amplification
- Building resilience amongst the target audiences of Russian disinformation across Europe
- Development of policy and resolve of government, multilateral institutions and tech companies to increase action to tackle disinformation

We will use the following performance indicators such as:

- Level of confidence in identifying and monitoring disinformation narratives
- Level of confidence in planning and executing counter disinformation campaigns
- Volume, frequency, quality and audience perceptions of campaigns
- % of instances of effective response to Russian disinformation campaigns
- Correlation of confidence levels and perceived campaign effectiveness with Network activities

- % of CSO partners sharing experiences, insights & learnings with Network peers

The data will be collected through:

- **Baseline Survey** run online with participating CSOs and demographically representative samples of the key audiences in Tier One countries/ organisations, as agreed with the FCO (500 respondents per country). The survey will gather attitudinal datasets, including towards Russia, disinformation and the media; and training needs (CSOs) and media habits (audiences). This survey will also provide a quick but comprehensive view of audience profiles for CSOs to target, and for the Network to measure the programme objectives against.
- **Quarterly Monitoring Surveys** with the same CSO and audience panels (where possible) to monitor changes in attitudes and perceptions. These will also provide a platform to test content concepts, and recall/perception of campaigns run in the preceding months.
- **Campaign Engagement Metrics,** collected by CSOs (following training), reported to their Network Manager and collated centrally (and securely) to improve peer to peer learning. The central M&E team will analyse samples of data to check for quality and assess what campaign re-adjustments are needed.
- **Language Analysis**, run by the central M&E team on samples of comments to understand sentiment towards and understanding of the topic of disinformation; adding value to strategy, content and programme evaluation. These codified comments will add qualitative insights to the evaluation of strategies, content and the programme overall.
- **Longitudinal Qualitative Panel (LQP),** a bi-annual study interviewing demographically representative samples of the target audience. Through in-person interviews in priority countries identified, over a period of six weeks, we will gain an in-depth understanding of the influence and persuasive power of (counter) disinformation narratives. These will inform future iterations of the programme and provide human insight into the impact of disinformation. The LQP will also provide valuable data to measure impact against our Theory of Change.
- **Peer to Peer Discussions,** taking place within the secure online forums and real-world events provided to Network Members. These will be both organic and facilitated, covering Network services, and the wider topics around disinformation. We will conduct discourse analysis on a quarterly basis to substantiate the survey data and in-depth interviews to provide context for the quantitative analysis and a wider breadth of qualitative data.
- **Stakeholder engagement and Monitoring**, to glean understanding of the policy and political developments to tackle disinformation, through scale. An indicative M&E framework is included below.

Evaluating activities against KPIs

Awareness, credibility and resilience towards disinformation narratives are subjective. So, the most effective way to monitor changes in attitudes (collectively or by sub groups of individuals) is to build a **Perceptual Impact Tracker.** From the statement responses (scored on a scale of 0 to 10) we will create an overall **Perceptual Impact** score, which can then be analysed over time, by different audiences and across different regions. We will create this for both key audiences identified and the CSOs, using data from the Baseline Survey as the foundation. Data from the Quarterly Survey will then be used against this to track shifts in perceived impact (up or down). To evaluate the role of the Network's activities in those changes, we will analyse correlations between the messages/training of CSOs and the resulting shift in perceptions, cross-referencing the **Perceptual Impact Tracker** with the data from the survey questions covering the volume and type of training received, grant funding received (for CSOs) and media/campaign recall for audiences.

Using Both Success and Failure to Improve Impact with CSOs

To ensure that the programme's overall objectives are met, we will build a **Reporting Process** that embraces the opportunity to reflect and learn as a collective through regular feedback loops. These will include understanding why and how campaigns were successful or not.

- **At the project level:** The results of the LQP, online surveys, campaign metrics and forum discussions will be accessible to CSOs and acting as both insight tool and training resource. CSOs will receive **mentoring and training** from the M&E team on the M&E methodologies (data collection, quality assurance, analysis) and how to use insight in communications planning. Peer-to-peer sharing amongst the Network, through sharing successes and synergies, will also provide valuable insights to tools and techniques. **A quarterly review process** by the M&E team will serve as a point of assessment where data will be analysed, adding to the mentoring methodology to support data analysis.

- **At the strategic level:** Audience-centric data and resulting analysis will be further captured in **Lessons Learned Reports** that the M&E team will prepare for the quarterly Project Board. Lessons learned Reports will be drafted in collaboration with Network Managers and will include proposed adaptations to programme activities as well as wider strategic programme recommendations to the Board (including reflection for HMG Enhance and Engage programmes). Following consensus by the Management Board and approval from the FCO, adaptations will be embedded into programme design for the next quarter.

- **At the Network Level**: There are three further ways we will capture learning throughout the project cycle and activity strands, to continually improve our approach: (1) capturing learnings at project level to shape the project strategy and regional strategies. This will be through weekly, monthly and quarterly reports against the KPIs and work through the Advisory Panel: (2) at the level of Network Members and Network Managers, aided through our self-perception tracker to adjust their activities accordingly: (3) At the sectoral level we will convene three policy roundtables each year with the aim of producing insights and developing best practice, norms and standards. Key industry, government, multilateral institutions, media and tech companies will attend, where lessons learned, and recommendations will be produced and disseminated as publicly available content, targeting expert and non-expert audiences. In year one, we will only host one event due to the shorter delivery timescale.

Responding to Poor Performance

To minimise and mitigate performance issues, across the project, we will co-create a **framework** at the start with the FCO and Network partners about **expectations, deliverables (KPIs), modes of communication, roles and responsibilities and escalation procedures**. This will inform project governance, quality controls and management. For this programme, project performance will be overseen by the Advisory Panel and Project Director, who will agree quarterly delivery targets with the Project Board, allowing for regular performance assessment against project plans, feeding into project KPIs. Ongoing data collection, including activity and outcome-level reporting, data analysis and lessons-learned will provide a regular flow of information to support performance tracking, using indicators set in the results framework. Performance against KPIs will be detailed in weekly, monthly and quarterly reporting.

We will deal swiftly and openly with poor performance, activating ZINC's poor performance procedures that aim to find active solutions quickly, to remedy any identified issue, including measures set-up in the inception phase that will include escalation to the FCO where necessary (if an issue is identified outside of regular reporting timetables). The following steps would be taken if underperformance against a KPI is identified: the Project Director will launch an issue tracker, that will set-out an agreed plan of action to rectify the issue, with activities mutually agreed, with the FCO, against milestones for completion. More detailed and regular reporting (outside of the weekly, monthly, quarterly timetable) would be activated, as a daily sitrep on progress against the issue (a particular KPI).

If a complaint is made about the Project Director, then the escalation process would be transferred to Louis Brooke, ZINC's Managing Director, as the owner of the procedures and the FCO's point of contact. This action would only be taken if Project Director contact – as a recipient of a serious complaint about conduct – was not feasible with the FCO. Louis Brooke would be supported by a relevant member of ZINC's Senior Management team, to offer a swift and comprehensive solution, activating risk mitigation plans in order that the Programme did not suffer as a consequence.

All underperformance of our sub-contractors in noted in Approach 1.6.

KPI Framework

		KEY INDICATORS	MEASURED BY	FREQUENCY	RESPONSIBILITY OF
IMPACT	Increased awareness of Kremlin disinformation amongst expert and non-expert audiences	Level of confidence amongst CSO partners to identify & counter	Perceptual Impact Tracker; Attribution Model	Baseline, then quarterly	Network M&E team
		Level of confidence amongst representative samples of the target audience to identify & ignore	Perceptual Impact Tracker; Longitudinal Qualitative Panel	Baseline, then quarterly; Bi-annual	
	Undermined credibility & reduced effectiveness of Kremlin disinformation campaigns	Level of confidence amongst representative samples of the target audience to identify & ignore	Perceptual Impact Tracker; Longitudinal Qualitative Panel	Baseline, then quarterly; Bi-annual	
	Level of confidence amongst CSO partners to plan & deliver counter campaigns	Level of confidence amongst CSO partners to identify & counter	Perceptual Impact Tracker; Correlation Model	Baseline, then quarterly	
		Level of confidence amongst representative samples of the target audience to identify & ignore	Perceptual Impact Tracker; Longitudinal Qualitative Panel	Baseline, then quarterly; Bi-annual	
	Development of policy and level of government, multilaterals and tech companies resolve to tackle disinformation increased	New policies adopted by identified stakeholders	Stakeholder Monitoring	Bi-annual	
		Strengthened policies / responses to disinformation	Stakeholder Monitoring	Bi-annual	
OUTCOME	Increased quality, quantity & effectiveness of counter-disinformation content	Volume, frequency & quality of CSO content as result of Network input	Correlation Model	Quarterly	Network M&E team
		Audience perception of the CSO content, likelihood to share with others	Campaign Engagement Metrics	Weekly update, monthly reporting	CSO partners
			Analysis of online comments	Monthly	Network M&E team
		% of instances of effective response to Russian disinformation campaigns	Campaign Engagement Metrics	Weekly update, monthly reporting	CSO partners
	Increased sustainability & professionalism of organisations countering disinformation	Level of confidence amongst CSO partners to design & execute strategies	Perception Impact Tracker, Peer-to-Peer discussions	Baseline, then quarterly; monthly	Network M&E team
		Correlation of CSO confidence to Network activities	Correlation Model	Quarterly	Network M&E team
	Creation of an ecosystem of credible voices to counter Russian disinformation	% of CSO partners active within the Peer-to-Peer forum & attending events; volume & variety of topics discussed	Peer-to-Peer discussions	Monthly	Network M&E team
	Established best practice for countering disinformation	% CSO partners sharing experiences, insights & learnings (successes & failures)	Peer-to-Peer discussions	Monthly	CSO partners
			Lessons Learned reports	Quarterly	Network M&E team
OUTPUT	Recruitment, training & mentoring of CSOs	Volume & type of training delivered		Weekly	Network M&E team
		Number of mentoring sessions attended		Weekly	Network M&E team
	Provision of peer-to-peer support & learning	Number of peer-to-peer events, numbers who attended		Weekly	Network M&E team
		Level of active participation in peer-to-peer discussions		Weekly	Network M&E team
	Training in data collection & development of an agile "make, measure, learn" culture	Volume, quality & frequency of data reports		Monthly	CSO partners
		Volume, quality & frequency of Lessons learned reports		Monthly	CSO partners