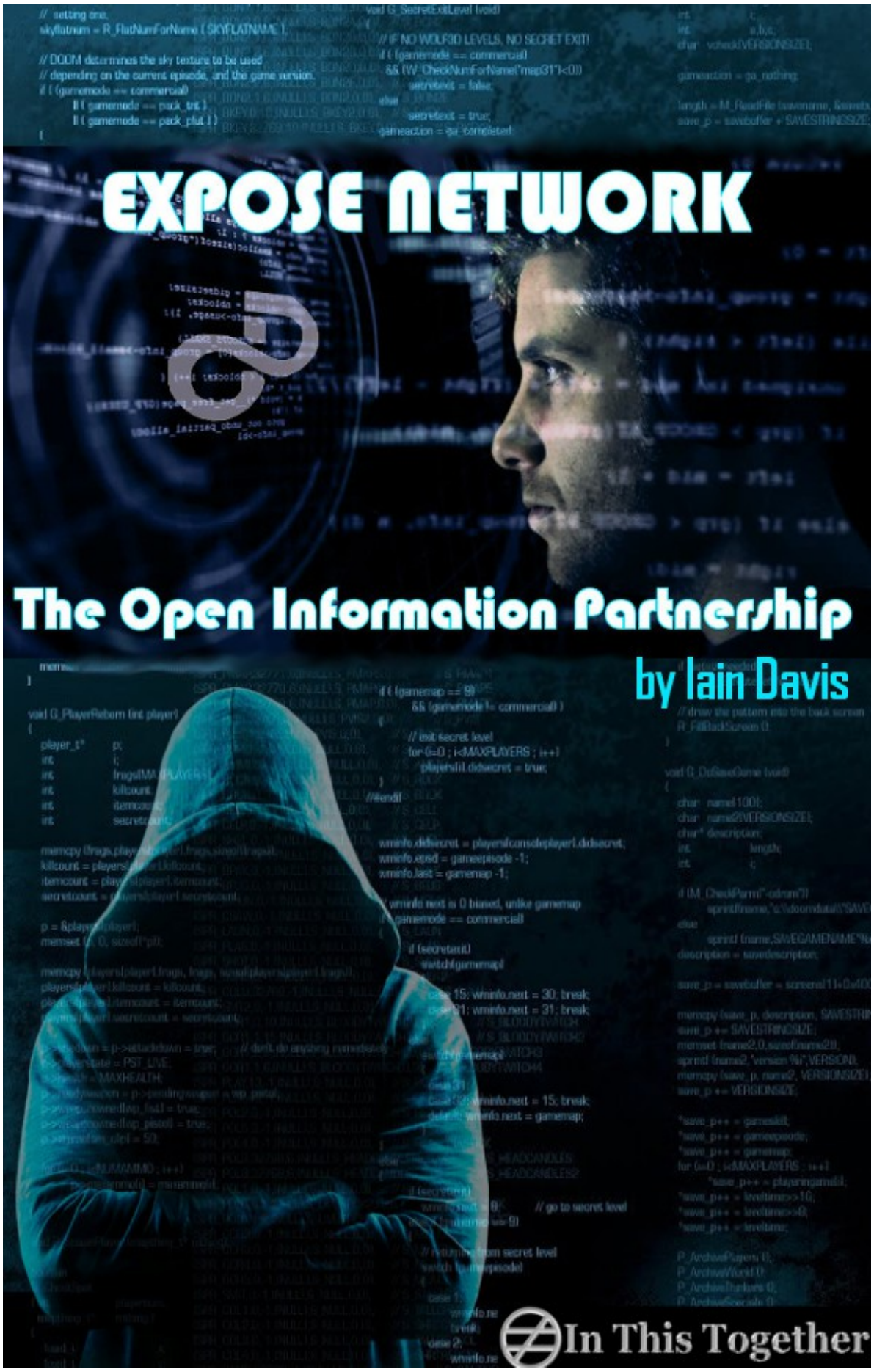

EXPOSE NETWORK
The Open Information Partnership
by Iain Davis
In This Together

The EXPOSE Network

An Open Information Partnership?

by Iain Davis

Formatted in the United Kingdom

First Formatted, 2019

www.in-this-together.com

Chapter 1: The EXPOSE Network & The Open Information Partnership

In this chapter we are going to consider an brief overview of the EXPOSE network. Further evidence and detail will be provided throughout this book. However I think there is some value to clarifying what we are talking about right from the start.

The EXPOSE Network (the name suggested by the FCO) is a project of the Counter Disinformation & Media Development Program (CDMD), currently headed by Andy Pryce. The likely contracting authority is the Secretary of State for Foreign and Commonwealth Affairs (then Foreign Secretary Jeremy Hunt). It is a £10 million tax payer funded 3 year project that was planned to run between Summer 2018 to 2021.

The Open Information Partnership (OIP) is the Network Hub of the UK Government Foreign and Commonwealth Office's (FCO) EXPOSE network. It is a one part of a wider UK/EU/NATO strategic communication and data gathering operation.

Andy Pryce: Head of the CDMD

We can rule out any idea the EXPOSE Network is genuinely concerned with *combating manipulated information*, as claimed by the OIP. At no stage, throughout its development, has any emphasis been placed upon investigation or the analysis of evidence. The attempts at uncovering genuine disinformation, which undoubtedly exists, have been distorted and exaggerated to such an extent, the findings are practically meaningless.

The Network Facilitator of EXPOSE is a consortium led by Zinc Networks who were formerly known as Breakthrough Media. The projects resource partners are Bellingcat, DFR Labs and the Media Diversity Institute. The implementing consortium partners are the Institute of Statecraft and Aktis Strategy (no longer operating) with risk management and security almost certainly provided by Toro Risk Solutions. Grant fund management is probably handled by Ecorys.

Both the EXPOSE network's and the larger EU/NATO strategic communications

(STRATCOM) operations are closely tied to globalist think tanks and multinational corporations. Its purpose is to promote EU/NATO policy objectives and undermine all who question them; it targets mainly European nations, especially in Eastern Europe and the Balkans but also others in Central Eurasia, almost certainly with a view to expanding towards North & Central Africa and the Middle East.

Its purpose is to control the flow of information, ensuring that public awareness is restricted only to official state narratives, in support of NATO/EU policy. In Part 1 we explore the social and political implications of the EXPOSE Network's propaganda.

The EXPOSE Network Revelations

Leaked documents reveal the purpose and scope of what we can call the EXPOSE Network, its facilitator (Zinc consortium) and its hub (the Open Information Partnership.) These documents are authenticated in Part 2 of the series. Following the leaks, a number of reports emerged. Many were from Russian state media outlets such as RT and Sputnik with others such as George Galloway and 21st Century Wire also drawing attention to the leaked documents.

We cannot be certain about the official name of this operation, or if it even has one. The only verifiable name is that given to the public facing element of its hub, the *Open Information Partnership*. However, as we shall see, the *'counter disinformation'* network proposed by the Zinc led consortium is active. The capabilities they offered the FCO in their technical proposal are deployed across Europe today. In the absence of any better term, we can refer to this project as

the EXPOSE Network. This was the original name suggested by the FCO.

It has been claimed that the planned EXPOSE Network hasn't reached fruition. The evidence revealed in this series of articles will show that it is currently operating at the heart of the European Union's *'Action Plan Against Disinformation'*. The threat it poses to democracy, freedom of speech & expression and the people's ability to openly and freely share information cannot be overstated.

It is clear that everything which challenges western state narratives is considered *Kremlin disinformation*. At no stage are the EXPOSE partners asked to consider the evidence substantiating this assertion. It is simply stated as fact.

Everyone who questions the policies, announcements and actions of EU/NATO aligned states are identified, by the EXPOSE network, as either willing or unwitting agents, assets, trolls or bots of the Kremlin. This includes, but isn't necessarily limited to, whoever the state decides is a far right or a far left group (no definition); people they consider anti-Zionists (no definition); anyone they label a conspiracy theorist (no definition); people who don't hate the Russian's, or *"Kremlin sympathisers"* as the FCO put it, (no definition); those who criticise the mainstream media (which appears to be just about everybody), fringe networks (no definition) and, even worse, fringe networks who share content using mainstream hashtags, resulting in unwanted information *"bleeding into the mainstream."* Twitter users basically.

Following the leak on 25th March 2019, on the 3rd April 2019, in response to a parliamentary question asked by SNP MP Stephen Gethins, then Minister of State and member of the parliamentary Intelligence and Defence Committee Alan Duncan, stated:

"We have a regular dialogue with international partners on the challenge posed by hostile state disinformation, including to align donor support in this field. The Foreign Secretary (then Jeremy Hunt) discussed disinformation at the EU Foreign Affairs Council on 21 January in the context of the European Commission's ambitious Action Plan Against Disinformation. The Foreign and Commonwealth Office's own dedicated Counter Disinformation and Media Development Programme aims to protect national security by countering disinformation directed at the UK and its Allies from Russia. It funds projects in a number of different countries that seek to enhance independent media, support civil society organisations that expose disinformation and share good practice with partner governments. Media plurality, institutional resilience and public awareness provide strong defences against disinformation, whatever the source, and sit at the heart of our efforts. **In**

particular, we are supporting a new Open Information Partnership of European Non-Governmental Organisations, charities, academics, think-tanks and journalists which are working to respond to manipulated information in the news, social media and across the public space.*"*

An undated draft proposal from the Foreign and Commonwealth Office (FCO) stated that the network (subsequently called EXPOSE) is a project of the CDMD program headed by Andy Pryce. It is inconceivable that he didn't at least authorise this draft. The proposed contract creates the role of a Network Facilitator to run the Network Hub of the EXPOSE network.

On 23rd May 2019, a promotional article for the OIP by Deborah Haynes, a named journalist in the UK cluster of the Integrity Initiative, confirms the details of a leaked draft of a £10 million contract over three years, with an anticipated roll out in the summer of 2018. The successful contractor is asked to *'assume'* independence.

In light of the level of direct CDMD control built into the leaked contract, this *'assumption'* appears to be little more than coded language for maintaining plausible deniability. It also identifies the EXPOSE Network as a priority for the CDMD.

Andy Pryce apparently attended a workshop discussing a network of NGO's on Wednesday 8th of August 2018 where he gave feedback on the terms of the contract. Zinc Network submitted their consortium bid to the FCO in a technical proposal dated 31st August 2018. So it seems likely that interested parties gathered to discuss the creation of the EXPOSE Network around late July to early August 2018.

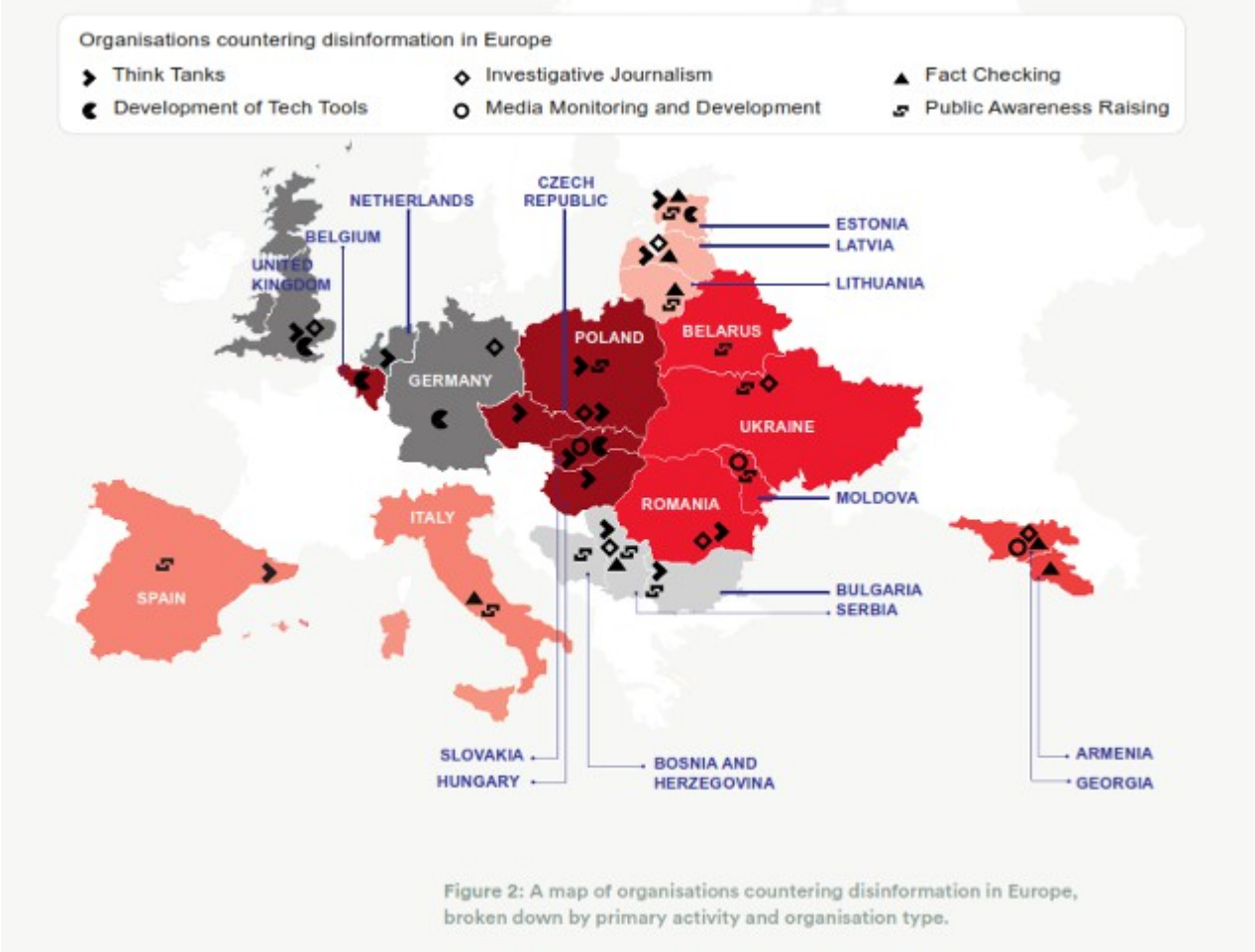


Figure 2: A map of organisations countering disinformation in Europe, broken down by primary activity and organisation type.

The current extent of the EXPOSE Network, with plans to expand

The EXPOSE Network Takes Shape

Shortly we'll assess the role of the EXPOSE Network Facilitator, operated out of anonymous offices in London by the Zinc led consortium (ZC). They demonstrate a number of capabilities including their skill at targeting individuals and intervening in election processes.

In June 2018, the CDMD issued their final scoping report for the the proposed EXPOSE Network. It established the role of a Network Facilitator to act as the central coordinator for the web of civil society organisations (CSO), non governmental organisations (NGO), fact checkers, smaller civil activists groups, journalists and bloggers across Europe and parts of Central Eurasia. The Network Facilitator would operate out of the Network Hub from where they could provide the technical & legal support, cyber & physical security, funding and training for the '*network of actors*.'

The Network Facilitator contract was won by a consortium led by Zinc Network. They submitted their technical proposal on or after the 31st August 2019. We can be reasonably certain this convinced the FCO to offer the Zinc consortium the contract. As with most contract bids, the FCO CDMD would have been interested to see what *'added value'* Zinc could offer them. We cannot be sure which elements of that added value the CDMD, who maintain close control of the EXPOSE Network, chose to adopt. We can be more confident about the elements the Zinc consortium are contractually obliged to deliver. These were specified in the scoping document and broadly outlined in the draft proposal.

The Network Hub is the Open Information Partnership, currently represented by nothing more than single page website. The webpage is essentially a ruse (disinformation) to sell the idea that the OIP is a public, open and transparent organisation. It meets the FCO's request that the operation be *'overt'* and no attempt be made to hide it. Like their suggestion that the Network Facilitator *'assume'* autonomy, this looks like an attempt by the FCO to maintain *"plausible deniability"*. Noting this desire, ZC addressed this in their technical proposal:

"*To be sustainable and less vulnerable to attack from malign actors, the Network needs to be public-facing…… the strategy for public facing communications is based on minimum requirements, such as a static website……..The project could expand to build on this public facing component, promoting the network as a journalist integrity and disinformation network……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.*

There is little doubt about the clandestine nature and precarious morality of the EXPOSE Network, openly addressed in numerous documents and evidenced by their present activity. In a bid to win the contract, ZC gave assurances to the FCO that their reputation would be protected:

"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 (the FCO CDMD)."

[Note: Bracketed information added.]

EXPOSE Networks Rapid Response

The Atlantic Council's DFRLab

Via their resource partners (Zinc Network, DFRLab, the Media Diversity Institute, Bellingcat) the EXPOSE Network is a *network of networks* drawing resources from governments, non governmental organisations, global corporations, wealthy philanthropic trusts, the international banking community, NATO and the EU. We look at the evidence substantiating this in Part 4 and Part 5. Key *supporting donor partners* include the National Endowment for Democracy, the Atlantic Council, The Open Society Foundation, USAID, NATO, the EU, Google, Facebook and Twitter among many others.

Advocating their *Rapid Response vehicle* the ZC offer the Counter Disinformation and Media Development Program the following service:

"….by coordinating members' (network of actors) 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…….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."

[Note: Bracketed information added.]

Speaking in June 2018, following the G7 summit, then UK Prime Minister Theresa May announced the G7's Rapid Response Mechanism. The G7 stated that hostile state activity will be met with a rapid and unified response. Alleged hostile states will be identified for their *'egregious behaviour'* and there will be swift, coordinated international attribution of guilt for cyber and other attacks.

Effectively they were declaring that foreign states will be blamed immediately for any event the G7 claims they are guilty of. No evidence or investigation required. Just arbitrary ascription of blame and rapid retribution. Apparently, this dangerous lunacy is part of the laboriously advocated *'international rules based system.'* It appears to differ somewhat from International Law which focuses more upon concepts shunned by the G7, such as due process and evidence.

The G7: Able to respond rapidly to whatever they like

It is now possible to envisage how the Rapid Response Mechanism will work from the public's perspective. The G7 will blame another country for some event or crisis. Currently this looks most likely to be Russia, Iran or China, but it could be any nation that falls into the G7's cross-hairs. Yemen maybe? Blame will be attributed without any investigation or need of proof. Evidence is irrelevant.

This will be accompanied by a slew of '*counter disinformation'* content pumped out by the EXPOSE Network. They will also rapidly identify anyone who questions the G7's assertion. The '*counter disinformation'*, accurate or otherwise, will support the G7 narrative without question.

Using the raft of Internet *'safety'* legislation currently being rolled out, EXPOSE Network *'supporters'* like Google, Facebook, Twitter and others, can then be directed towards shared information contradicting the G7's assertions and purge the offending accounts. Along with all information, including any evidence, they

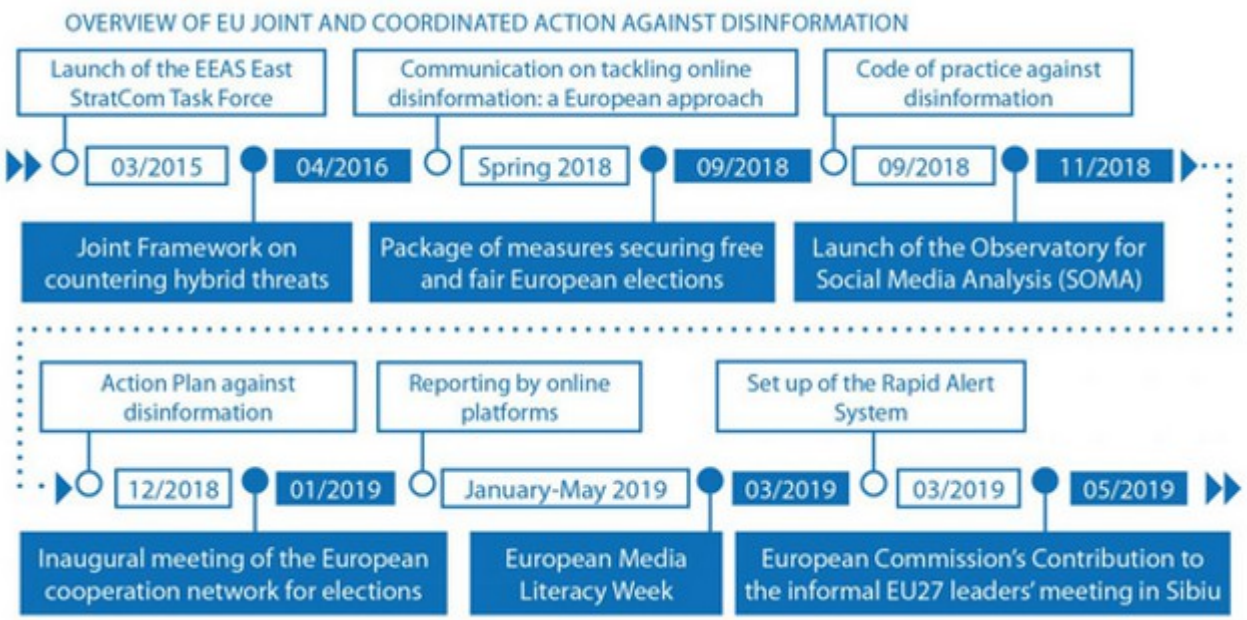
direct the public towards. The Internet, as we know it, is increasingly being controlled. Access to information will be limited by the state and their corporate partners.

EU Evidence of the Threat Level

There were some other notable components of Alan Duncans announcement of the Open Information Partnership. He stated:

"We have a regular dialogue with international partners on the challenge posed by hostile state disinformation…….The Foreign Secretary discussed disinformation at the EU Foreign Affairs Council on 21 January in the context of the European Commission's ambitious Action Plan Against Disinformation"

The EXPOSE Network sits within "*the context of the European Commission's ambitious Action Plan Against Disinformation*." Duncan's statement alone is far from the only reason to believe this the case.



The EU Action Plan Against Disinformation, spells out the evidence it has based a planned €123 billion investment upon. This investment is to enhance the capabilities of the European External Action Service (EEAS) with a particular focus upon SRATCOM capability. This evidence is provided by the EEAS team called the East StratCom Task Force (ESTF). The EU state:

"The East Strategic Communications Task Force, has catalogued, analysed and put the spotlight on over 4,500 examples of disinformation by the Russian Federation, uncovering numerous disinformation narratives…."

The Easta StratCom Task Force' (ESTF) main method for countering disinformation is *'raising awareness'* about it via their weekly *Disinformation Review.* The full record of the Task Force's work on disinformation is available on the ESTF's own EUvsDisinfo website.

East StratCom Task Force website

The work of EUvsDisinfo is central to the EU Action Plan. It provides the evidence which informs the EU's assessment of the *Russian disinformation* threat. The influential U.S. think tank and policy advisors, the German Marshall Fund, wrote a policy paper in August 2019. They observed:

"EU vs Disinfo's research and documentation efforts were instrumental in changing the debate about Russian disinformation and hybrid threats within the European Parliament and EU institutions."

The *full record* of the 4,500 examples of disinformation, rather than emanating from academic or intelligence based assessments, are the sum of EUvsDisinfo's Open Source Intelligence (OSINT) informed *'weekly reviews.'*

In Part 6 we examine this claimed evidence. Time and time again, when you check the links alleging Russian disinformation, proof either doesn't exist or is spuriously contrived from entirely subjective interpretations of mainly MSM content. Hard evidence, proving the scale of this fabled Russian disinformation operation, doesn't exist.

In March 2018 the ESFT were forced to issue a retraction after three Dutch media outlets threatened to sue them for falsely labeling them as *'disinformation.'* The ESFT acknowledged the Dutch were right and claimed they were *"taking steps to further improve."*

In fact, the ESFT don't seem to have much faith in their own investigations. Carefully adding a disclaimer to every *'Disproof'* stating:

"This does not necessarily imply, however, that a given outlet is linked to the Kremlin or editorially pro-Kremlin, or that it has intentionally sought to disinform."

Posing the question, if it implies the story is neither linked to the Kremlin nor that it is pro-Kremlin and it doesn't intentionally seek to *'disinform'*, how can it possibly be '*Kremlin disinformation'*?

As with the EXPOSE Network, it seems the EU's assertion, regarding the scale of Russian disinformation and the level of threat it presents, is fallacious. It is as if they are reading from the same script.

EXPOSE Network Provide the Evidence

We know that one of the EXPOSE Networks recommended *'fact checkers'* is the Ukrainian based StopFake. They report:

"Britain is thought to be leading [the] EU in building a grassroots campaign against

Russia's attempts [disinformation]. The campaign is lead by the Foreign and Commonwealth Office and executed by a communications agency called Zinc Network."

[Note: Bracketed information added]

EXPOSE Network *'actor'* the European Values Center

Certainly when we look at the EXPOSE Networks *'actors'*, that appears to be the case. Of these, perhaps one of the most influential is the European Values Center for Security Policy. Through them we can see how the transatlantic NATO/EU EXPOSE Network operates. Their two biggest funders are the Dutch government and the UK Foreign and Commonwealth Office.

One of European Values' projects is Kremlin Watch, which claims to tell you *"everything you need to know about about Russian influence operations in Europe."* They also tell us quite a bit about the role of the EXPOSE Network in Europe. They state:

"Our team is the most active contributor to the EEAS East STRATCOM network (ESFT), which produces the Disinformation Review."

[Note: Bracketed information added]

It seems the EXPOSE Network is providing the *Kremlin disinformation* analysis, via the East StratCom Task Force, which the European Union are using to justify draconian Internet regulations and planned tax expenditure of €123 billion over five years. The quality of that analysis appears to be so poor we might consider if it is itself '*disinformation.*' The Action Plan builds upon the work of the ESTF, which is the work of the EXPOSE Network.

The EXPOSE Network is an operation of the Counter Disinformation and Media Development Program of the UK Government Foreign and Commonwealth Office (FCO). This suggests the UK Government are working with the European Union to create a €123 billion tax payer funded budget, based upon their own highly questionable *Kremlin disinformation* analysis. A healthy return on an initial £10 million investment. What really matters is that the tax paying public believe the threat is real.

As long as they do they will accept the imposition of restricted online freedoms and won't resist the NATO/EU joint policy to control all information. The EXPOSE Network's resources are not limited to official budgets and direct political oversight is limited. It partners with a huge network of global interests each seeking, both individually and collectively, to benefit from the EXPOSE Network's capacity to influence NATO and EU policy. It is at the heart of the European Union's STRATCOM strategy and uses manipulated information to mislead, misdirect and misinform both policy makers and public alike.

Its existence is anti democratic and its activities demonstrate total disregard for the principles citizens in western democracies hold dear. If it is all it claims to be then it should not fear scrutiny. It should be as open and transparent as it promises on its single page website and genuinely engage with the public's

questions, born from the critical thinking it allegedly venerates.

It is an immense threat to free speech and freedom of expression. Each an every one of us needs to exercise our rights, and demand the EXPOSE Network account for itself.

Chapter 2: An Introduction to the EXPOSE Network

A multinational, state backed, corporate funded, information control and censorship network is operational in Europe and beyond. The threat it poses to democracy, freedom of speech & expression and the people's ability to openly and freely share information cannot be overstated.

Leaked documents reveal the purpose and scope of what we can call the EXPOSE Network, its facilitator (Zinc consortium) and its hub (the Open Information Partnership.) These documents are authenticated in Part 2 of the series. Following the leaks, a number of reports emerged. Many were from Russian state media outlets such as RT and Sputnik with others such as George Galloway and 21st Century Wire also drawing attention to the leaked documents.

We cannot be certain about the official name of this operation, or even if it has one. The only verifiable name is that given to the public facing element of its hub, the *Open Information Partnership*. However, as we shall see, the *'counter disinformation'* network proposed by the Zinc led consortium is active. The capabilities they offered the FCO in their technical proposal are currently deployed across Europe, especially the Eastern Partnership. In the absence of any better term, we can refer to this project as the EXPOSE Network. This is the original name suggested by the FCO.

It has been claimed that the planned EXPOSE Network hasn't reached fruition. The evidence revealed in this series of articles will show that it is presently

operating at the heart of the European Union's '*Action Plan Against Disinformation'*. It is clear that everything which challenges western state narratives is considered *Kremlin disinformation*. At no stage are the EXPOSE partners asked to consider the evidence substantiating this assertion. It is simply stated as fact.

The EXPOSE Network & The Open Information Partnership

The EXPOSE Network is a project of the Counter Disinformation & Media Development Program (CDMD), currently headed by Andy Pryce. The likely contracting authority is the Secretary of State for Foreign and Commonwealth Affairs (then Foreign Secretary Jeremy Hunt). It is a £10 million tax payer funded 3 year project that was planned to run between Summer 2018 to 2021.

The Open Information Partnership (OIP) is the Network Hub of the UK Government Foreign and Commonwealth Office's (FCO) EXPOSE network. It is a one part of a wider UK/EU/NATO strategic communication and data gathering operation.

We can rule out any idea the EXPOSE Network is genuinely concerned with *beating manipulated information,* as claimed by the OIP. At no stage, throughout its development, has any emphasis been placed upon investigation or the analysis of evidence. The attempts at uncovering genuine disinformation, which undoubtedly exists, have been distorted and exaggerated to such an extent, the

findings are practically meaningless.

Investigative journalism is denounced as expensive and impractical, reporting verifiable evidence isn't mentioned, and seeking recourse via international law is notable only by its absence. *Counter disinformation* is a transparent cover term for propaganda.

The Network Facilitator of EXPOSE is a consortium led by Zinc Networks who were formerly known as Breakthrough Media. The projects resource partners are Bellingcat, DFR Labs and the Media Diversity Institute. The implementing consortium partners are the Institute of Statecraft and Atkis Strategy (no longer operating) with risk management and security almost certainly provided by Toro Risk Solutions. Grant fund management is probably handled by Ecorys.

Both the EXPOSE network's and the larger EU/NATO strategic communications (STRATCOM) operations are closely tied to globalist think tanks and multinational corporations. Its purpose is to promote EU/NATO policy objectives and undermine all who question them; it targets mainly European nations, especially in Eastern Europe and the Balkans but also others in Central Eurasia, almost certainly with a view to expanding towards North & Central Africa and the Middle East.

Andy Pryce: Head of the CDMD

Its counter disinformation is based upon the assumption that anything and everything which challenges either EU/NATO policies or narratives are products of *Kremlin disinformation*. This is a *'threat to national security'* and is therefore to be opposed. Those who challenge western state narratives or criticise policy will be identified and reported as Kremlin disinformation agents, assets, trolls or bots to the Counter Disinformation and Media Development Program (CDMD) of the UK Government Foreign and Commonwealth Office.

The EXPOSE networks STATCOM (a common euphemism for propaganda) activities are tied in with the raft of internet regulations being created by European states. These include the UK's proposed Online Harms legislation and the EU's recent copyright directives. Google, Facebook, Twitter and other 'tech giants' are both backers of, and in some cases likely involved in, the EXPOSE Network's operation.

It is these global corporations and Social Media giants who will be tasked, under the new Internet regulations, with applying the necessary *'rules'* to ensure those identified as peddling Kremlin disinformation are effectively silenced online. The *network of actors*, directed by the CDMD, will also be supported to lobby for further regulation of the Internet.

The Implications of the EXPOSE Network

This article is 1 of 6 examining the web of western governments, Civil Society Organisations (CSO), Non Governmental Organisations (NGO), journalists & smaller scale actors, bloggers and activists who form the EXPOSE network. As I'm sure you've figured out by now, there's a lot of detail to cover. Please stick with it, if you can make the time. I think you will find it worthwhile.

We will also consider how the EXPOSE Network is embedded, throughout Europe and central Eurasia. We'll look at who is funding the operation, some of their history, motives and objectives. We will examine the evidence, cited throughout, which prompts reason for concern.

Before we do, let's briefly think about the implications suggested by the EXPOSE Network. Leaked documents reveal its true purpose and scope, its facilitator (Zinc consortium) and its hub (the Open Information Partnership.) In Part 2 we'll authenticate those documents. For now, let's just consider what they say.

The EXPOSE Network document Upskilling and Upscale: Unleashing the Capacity of Civil Society To Counter Disinformation defines disinformation as:

"Kremlin influence operations within the communications environment."

The examples cited are:

"Smear campaign against the White Helmets, a group trusted by the UK government, especially their evidence of the use of chemical weapons by Russia and its allies in Syria."

And:

"Creating multiple false narratives to reject the UK Governments analysis of the poisoning of the Skripals in Salisbury or muddying the waters around the shooting down of the MH17 airliner by Russian controlled forces in the Ukraine."

Aside from the fact this appears to confirm the UK Government's *'open source intelligence'* (OSINT) on alleged chemical weapons attacks in Syria came from the White Helmets and they believe Russia, not just the Syrian government, were responsible, this definition raises other concerns.

This investigation is not about me, but perhaps some self disclosure is pertinent. I am one among many who have questioned the Skripal narrative, the Syrian chemical weapons attack claims and the role of the White Helmets. I'm a British citizen, I don't know any Russians and I don't support the Russian state. I don't believe the Russian mainstream media (MSM) any more than I believe the western MSM. Nor do I unquestioningly accept reports by the so called *'alternative media.'* I don't claim to represent anyone else's views, but I know my experience and approach are fairly common.

Defending media freedom?

My initial suspicions about these official state narratives were alerted not by others opinions but rather by noticing the apparent lack of any verifiable evidence supporting them. MSM reports that *"experts say"* or *"intelligence sources confirm"* are not sufficiently convincing for me. When I see such phrases, I want to know more.

Like millions of others, before believing something I'm told I want to see the actual evidence to properly inform my opinion. Especially if the public, myself included, are then invited, usually by the ubiquitous MSM, to rally behind a state policy to blame a foreign power or launch military action as a result. Apparently, in accordance with the OIP's own statements, an informed public is also something of great importance to the EXPOSE Network.

When researching these events I used a variety of information sources. Mainly western based mainstream media, official government and NGO reports, political and official statements, alternative media (fellow bloggers and websites) and books, freely available for purchase in the UK. All of it in the public domain. My motivation has always been to understand as much as I can about world events

and share my perspective. Like anyone else I have cognitive bias, but I try to stay as objective as possible and focus on evidence.

I'm not so interested in opinion but rather cited primary and secondary sources where I can read information, eyewitness accounts, official reports and so on for myself. I reserve the right to make up my own mind.

In general I find the *'alternative,'* or rather *'independent'* media better at citing their sources than the MSM. They tend to be more useful from a research perspective, simply for this reason. However, the MSM also provide valuable information. It just requires additional research to track down their sources. There are still a dwindling number of decent journalists working in the MSM. While I am critical of the MSM as a whole, I do not suggest it is useless.

I strongly support the notion of a truly independent media, investigating powerful influences and forces. Given their resources, it would be preferable if the MSM applied themselves to the task and gave greater prominence to journalists who question power. They don't appear too inclined to do so and a vacuum has been created which has been filled by others.

Unfortunately, when former UK Foreign Secretary Jeremy Hunt spoke about *independent media* at the Global Conference for Media Freedom his version of an *'independent media'* was the media, either owned by a handful of global corporations or state run, which doesn't question power.

A truly independent, subscriber supported, investigative media has been flourishing online. If Hunt was serious about media freedom then it is this small cottage industry of shoestring teams of investigative reporters he should encourage, alongside the established MSM. They would undoubtedly benefit from

resources, legal advice and technical support.

Market competition is surely what a free market economy is all about? Do we live in one or not? However, rather than support them, Hunt is among those who see them as a '*threat to national security*'.

Independent or 'alternative' media? A threat to national security?

This is not based upon the quality of their work, which often exceeds the MSM's, but rather their subject matter. It appears *'independent media'* is defined by the UK Government solely as those who unquestioningly support EU/NATO policy and have the corporate or state resources to promote it.

Thanks to the Internet, with sufficient time and interest, anyone can do their own research, look at the evidence and make up their own mind. They don't need to be told what *'the truth'* is by anyone. This, I suggest, is the real problem the EXPOSE Network and its OIP, among others, have been tasked to combat.

If the EXPOSE Network's definition is to be believed then I, thousands of others and all of these sources, including the MSM and official government reports, are *Kremlin disinformation*. Which means that the Kremlin are running by far the most powerful, expensive and all pervasive propaganda operation in history. Despite the fact NATO and U.S combined defence spending is more than 25 times greater than Russia's. We will see that the EXPOSE Network has consistently failed to provide plausible evidence to validate their claims about the scale of this alleged *Kremlin disinformation* program.

Reasons for Concern

The notion that all who question the UK government's official accounts are, by definition, Kremlin disinformation agents is not only absurd it is antithetical to both free speech in a democracy and the essential function of a genuinely free and open press to question power. Many in the so called *'alternative media'* predominantly question Western power. These mainly U.S. and West European outlets do so, not because they favour Russia, China or Iran (for example) but because they are citizens of western democracies holding their own elected governments to account. As is both the supposed purpose of the media and everyone's right in alleged democracies.

Some will say this shows bias, but those of us who live and work in the West aren't subject to the laws, social contracts and taxation of Moscow, Beijing or Tehran. Citizens in the West are subject to the rule of western governments and they exercise power in our names. The onus to hold this power to account is upon us. We can't expect the Russians to do it for us. This doesn't mean the *'independent media'* aren't, for example, critical of Russian or Chinese policies. Asking questions of your own government does not signify support for another.

State funded broadcasters, such as RT, al Jazeera, the BBC and the USAGM global media network do periodically spread state propaganda, and disinformation. All governments use compliant media outlets in this way. This doesn't mean that state funded broadcasters report nothing other than propaganda, but they are available to disseminate it when required. Recent history is littered with examples of Western states deliberately using the mainstream media (MSM) to mislead the public, cover up wrongdoings and use propaganda to sway public opinion.

For example, state disinformation underpinned the mainstream media narrative which provided former UK Labour Prime Minister Tony Blair, allied with then U.S. President George Bush, the necessary political clout to launch the illegal Iraq War in 2003. A war that killed millions, destabilised the Middle East, created the conditions for the further spread of terrorism and led to increasing hostilities which now appear ominously close to starting another major conflict. With a few notable exceptions, the Iraq war is now almost universally acknowledged as an avoidable disaster.

Hyde Park 15/02/2003 – An Estimated 6M people marched across the world.

Millions of people protested the decision to go to war with Iraq. They marched through cities across the western world imploring the lunatic fringe of neocons and war-hawks to halt what they knew was a war of conquest founded upon lies and disinformation. Yet even this unprecedented level of public outcry failed to impact upon the decision makers we elect. Ably assisted by the mainstream media, any narrative, no matter how doubtful, can be sold to a largely misinformed *'silent majority'* through the use of propaganda and disinformation.

Labeling all dissent *Kremlin disinformation* appears to be a deliberate ploy to silence any criticism of EU/NATO aligned policies. In doing so it utterly destroys the founding principles of our society. That of every citizen's equal right to freedom of speech, expression and free & open access to information. Including the right to cite evidence justifying their disagreement with state policies.

These are not rights we should casually toss aside in the name of national security. If national security requires that the people themselves are effectively labelled enemies of the state, simply because they disagree with it, then we must ask whom *national security* is intended to protect. Because it doesn't appear to be

the ordinary citizen. If such actions prevail, how can any of us consider the state a democracy?

The Purpose of the EXPOSE Network

The EXPOSE network is an attempt to ensure that the likes of the huge 2003 anti-war protests, propelled by public awareness of evidence presented by people like Hans Blix and Dr David Kelly, never happen again, especially online. Such a groundswell of disparate individuals sharing relevant material, evidence and opinion via the Internet could quickly overwhelm the more limited information strangle hold of the mainstream media.

In isolation, street protests, no matter how large, can be side-lined or downplayed by the MSM. Wider public opinion can be controlled to a certain extent. Modern communication technology has changed that. The state has found itself unable to muster the kind of all-encompassing propaganda it deployed in 2003 to drive the decision to go to war with Iraq.

A recent example of how states, or elements within states, have lost narrative control was the U.S. national broadcaster A.B.C's *'fake news'* story on Turkish forces allegedly attacking Kurds in Northern Syria. ABC repurposed 2017 footage from a night fire demonstration at the Knob Creek Gun Range in Kentucky, citing it as primary evidence (on the ground footage) of what they called the Turkish *"slaughter in Syria."* Thanks to the Internet, ordinary people quickly identified and exposed this propaganda, forcing ABC to issue a retraction.

Had this occurred prior to the Internet age, it is unlikely the disinformation would have been revealed. Those who noticed the deception could have easily been dismissed as cranks, conspiracy theorists or *Kremlin disinformation* assets. ABC's

fake news could then be cited as *'evidence'* by others supporting the promoted narrative.

The Internet meant proof of the deception was shared globally in a matter of hours. It quickly achieved viral reach simply because sufficient numbers of people were interested enough to share it. Faced with this technological reality, the MSM can no longer hide the full extent of its disinformation. Its credibility, and propaganda value to the state, has waned markedly as a result.

The ABC debacle is just one of thousands of examples of western MSM disinformation which *'citizen journalists'* have been able to prove beyond reasonable doubt. Among the most egregious of these was the BBC's 2013 documentary 'Saving Syria's Children.' Thanks to the diligent research of Robert Stuart the evidence that the BBC faked footage of the medical response to an alleged attack on a Syrian playground is overwhelming. Especially in light of the BBC's failure to adequately address any of the evidence.

The Great Fear Driving the EXPOSE Network

Are you the threat to national security?

The EXPOSE network is just one part of a concerted effort by all states, including Russia, China and other nations, to regain control of information. The current iteration of the Internet empowers the people. This is clearly seen as a problem by the holders of power, wherever they may be.

Consequently, in the West, highlighting U.N weapons inspector's opinions or their engineering assessments, which challenge the state's version of events, is now defined as *Kremlin disinformation*. For its part, the Kremlin deem criticism of the state to be bad form. Its the same game, just a different tactic.

Despite the MSM's apology for their Iraq war propaganda' the MSM's overall standards haven't improved. Since 2003 there hasn't been a single western military intervention they haven't thrown almost their entire weight behind. Those few MSM journalists who do question power have found it increasingly difficult to get stories passed their editors. If they do, they rarely make the headlines.

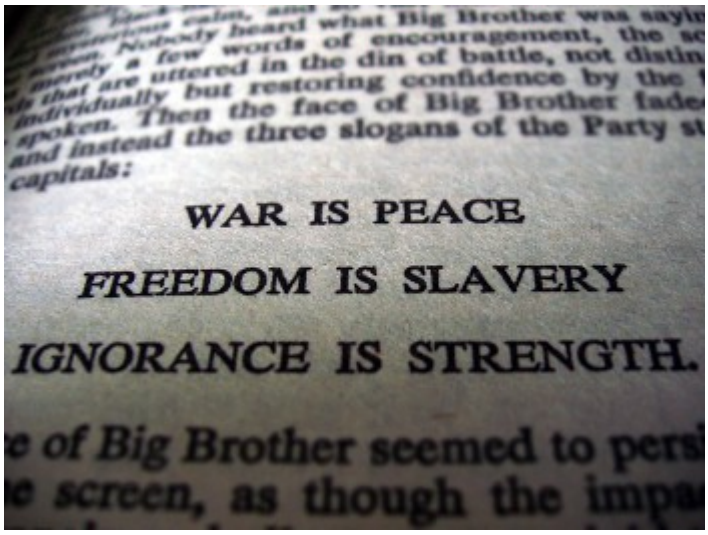
Having seemingly learned nothing, far from questioning official narratives, as a whole the MSM unfailingly support and promote them. Contradictory evidence, available in the public domain, should prompt the MSM to do their job, investigate and report it. Yet they consistently divert the public's attention away from the evidence, primarily by insisting that the those who highlight it are crazy conspiracy theorists or *Kremlin disinformation* assets.

The Internet had made it possible for ordinary citizens to research the issues that interest them. If inclined, they can then create blogs, videos, podcasts, memes and more and then share their opinions with their fellow citizens on a previously

unimaginable scale. Predominantly by using social media. That time is rapidly coming to an end.

Some, but far from all, of this content is ill informed, based upon poorly referenced sources, driven by political or social agendas or even influenced by genuine *Kremlin* disinformation. However, this is an unavoidable consequence of free speech in an open and free society. The alternative, adopted by the EXPOSE network, is to attack everything that questions the state.

All of us are wrong at times. As I am undoubtedly about to prove. This is nothing to fear. Responsible adults are capable of critical thinking and due diligence is within everyone's grasp. I urge you to read these posts with a critical eye. I have no special insight into *'da troof.'* Discovering we are wrong is an essential part of the learning process. If the only information we access simply reinforces our existing beliefs, never challenging them or offering an opposing view, then we learn nothing.



Orwell's warning wasn't a suggestion.

If the state effectively eradicates all information which questions it, in an effort to police the tiny proportion that is a result of foreign state disinformation, all the people will have left is the official opinion of the state. Orwell tried to warn us about this, he wasn't suggesting it as a policy. The EXPOSE network is taking a sledge hammer to crack a nut. We would be foolish to ignore the possibility that this is deliberate.

Rather than just marching in the streets, the people can now communicate directly with their elected representatives on an almost daily basis. What's more, others can see the questions asked and note the responses, or lack of them. Lobbying politicians and decision makers is no longer the sole province of those with deep enough pockets to afford it. This too is apparently a threat to *national security*.

Online communication comes with some risks. Public figures, like anyone else, deserve protection from harassment and threats. We need to carefully balance people's individual safety, especially the safety of children, with the right to freedom of speech and expression. Unfortunately, the state appears to be exploiting this concern, absent any genuine debate, as a justification for draconian Internet regulation and online STRATCOM operations.

Baseless State Censorship of the Internet

In its current form the Internet has the potential to transforms political accountability far beyond the ballot box. It is essentially nonviolent and offers the possibility of an informed citizenry asking the questions of power that the MSM have largely failed to do. The people can form their own lobby groups, generate

petitions compelling debate (in theory) and raise awareness of issues important to them.

The Internet is undoubtedly the most democratic of innovations. Yet all we see from the state are continual attacks upon it and demands to regulate, legislate and curtail the freedoms it affords.

We are constantly told how 'fake news' and Kremlin disinformation threatens our democracy, our children, our *'way of life.'* We are inundated with MSM stories about how the Internet radicalises people to commit violent acts, even acts of terrorism. It is as if terrorism and violence never existed prior to the Internet age.

Those of us old enough to remember the horrors of Omagh, Birmingham, Guildford and elsewhere should perhaps inform those who aren't of some uncomfortable truths. Outrages like the Manchester Arena bombing or the Christchurch shooting are not the product of online disinformation. The root causes are far more complex.

Terrorism and the deranged acts of mad men have existed for thousands of years. They have not suddenly become worse, or more prevalent, because of the Internet. No matter what the state and the MSM claim.

However, the message we are given to believe is clear. The Internet, the open and free sharing of information, is dangerous and something must be done. We need to ask, dangerous for whom?

The EXPOSE network is part of a much larger transatlantic movement aiming to silence all criticism of western state policies, actions and narratives. *Kremlin disinformation* can be absolutely anything at all. From questioning vaccine safety

to climate science, raising concerns about western state reports of major events, exposing government corruption, critiquing western policy or military action. All is deemed *Kremlin disinformation*. Whether it is or not.

No evidence is required to validate the *Kremlin disinformation* assertion. Whatever the criticism may be, no matter who makes it, if not approved by the state, it will be labelled as such. The EXPOSE network is self-referencing, its own unsubstantiated propaganda can be cited as 'evidence' to support further propaganda. It is rings within rings exemplified.

Moving Forward

Sir Nick Carter thinks he's at war.

Though we may not know it, we need to understand we are in an information war. Recently the British Chief of Defence Staff Sir Nick Carter, sharing a platform with the former Director of the CIA, told the Cliveden set:

"The changing character of warfare has exposed the distinctions that don't exist any longer between peace and war….I feel I am now at war, but it's not a war in the way we would have defined it in the past. And that is because great power competition and the battle of ideas with non-state actors is threatening us on a daily basis…….The character of warfare is evolving…..Information is going to be at the core of so much that we do. Future warfare is going to be very much information-centric…."

Apparently war and peace are the same and non state actors (people) are the enemy. We have had no political debate about this redefining of warfare but, as far as the head of British defence and security forces understands, that's just the way it is. The new battleground is cyberspace and the information sphere.

This notion of perpetual hybrid war can arguably be traced to former U.S. President Reagan's 1982 Westminster Address. It is certainly evident in Theresa May's vaunted Fusion Doctrine. The people didn't ask for this but it has been foisted upon them by the state.

Prior to the Internet, control of reported information was, by and large, relatively easy for the state. Some careful manipulation of the mainstream media, the odd D-Notice thrown in, and all was as it should be.

Our use of the Internet has transformed the information landscape and we are now far less reliant upon single sources of information. The daily paper has been replaced by the daily scroll through our news feeds. The traditional television and

newsprint media are losing their audiences and revenue. State control of information has diminished as a result. It wishes to reassert it. Non state actors are their target.

We should be under no illusions. Our online freedoms are under heavy and sustained attack. If we consider online freedom of speech and expression to be an important part of our modern democracy then, by implication, democracy itself is also under attack. Perhaps it always has been.

With that in mind, in the next chapter we'll start looking at the recent leaked information which uncovers the EXPOSE network and the Open Information Partnership.

Chapter 3: Examining the Role of the EXPOSE Network

We've looked at the EXPOSE Network and its Hub, the Open Information Partnership (OIP). As a counter disinformation project of the UK Foreign and Commonwealth Office's (FCO) Counter Disinformation and Media Development Program (CDMD), we discussed the potential implications of its activities. Much of what we know about the OIP and EXPOSE came from a documents leaked by the group Anonymous (via CyberGuerilla) as round 7 of the Integrity Initiative leaks.

We can't be certain who leaked these documents so some scepticism is warranted. However, we can establish their veracity by corroborating them with information available in the public domain. A simple search of the Internet archive proves these documents were online before the 26th March 2019. At that

time, there was no other publicly available information concerning the EXPOSE network. There remains little today.

Verifying EXPOSE Network Document Authenticity

Following the leak, on the 3rd April 2019, in response to a parliamentary question asked by SNP MP Stephen Gethins, then Minister of State and member of the parliamentary Intelligence and Defence Committee Alan Duncan, stated:

"We have a regular dialogue with international partners on the challenge posed by hostile state disinformation, including to align donor support in this field. The Foreign Secretary (then Jeremy Hunt) discussed disinformation at the EU Foreign Affairs Council on 21 January in the context of the European Commission's ambitious Action Plan Against Disinformation. The Foreign and Commonwealth Office's own dedicated Counter Disinformation and Media Development Programme aims to protect national security by countering disinformation directed at the UK and its Allies from Russia. It funds projects in a number of different countries that seek to enhance independent media, support civil society organisations that expose disinformation and share good practice with partner governments. Media plurality, institutional resilience and public awareness provide strong defences against disinformation, whatever the source, and sit at the heart of our efforts. **In particular, we are supporting a new Open Information Partnership of European Non-Governmental Organisations, charities, academics, think-tanks and journalists which are working to respond to manipulated information in the news, social media and across the public space**."

[Note: Bracketed information and highlighting added]

Alan Duncan M.P

Duncan's statement was soon followed, on the 4th April, by an enthusiastic tweet from Bellincat, who are one of the resource partners of the Zinc consortium who obtained the contract to act as EXPOSE Network facilitators. Bellingcat now openly declare their membership of the OIP on their website. Again, an archive search shows this information did not appear on the Bellingcat website prior to the 8th April 2019. Similarly, there is no record of the OIP website being online before the 4th April 2019.

On the 23rd May, two months after the document leak, Deborah Haynes, a journalist listed as a member of the Integrity Initiative UK Cluster, wrote a promotional article for the OIP published by Sky news. This is the first time information on the value and duration of the OIP contract, along with some further details, were released to the public. In this instance by the mainstream media (MSM.) Haynes confirmed the following:

- A £10 million programme

- 3 year Contract

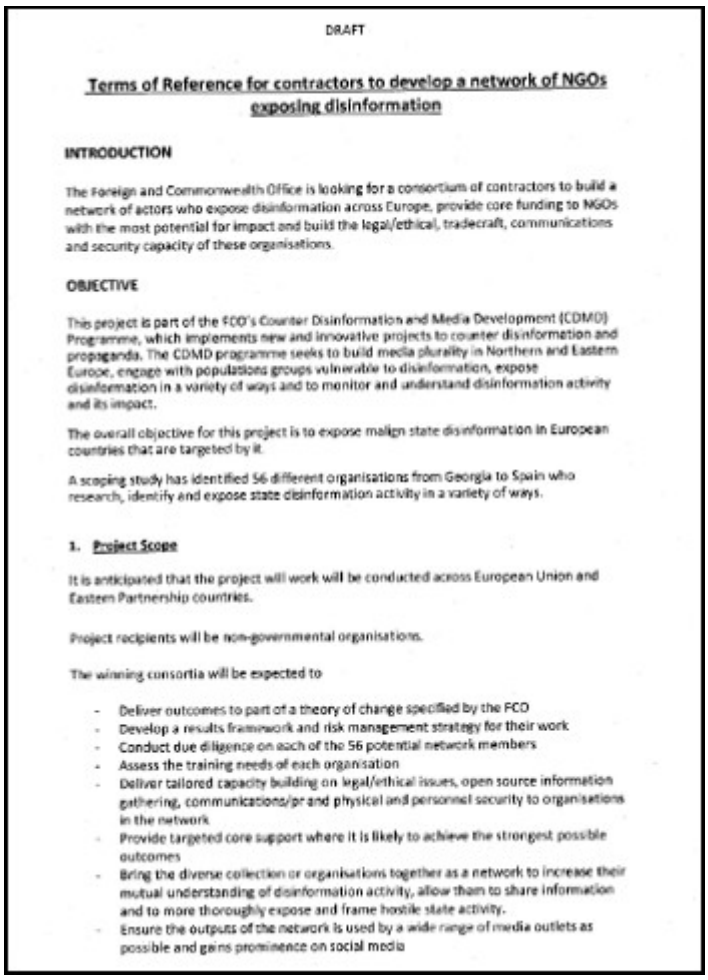
- Provides grants to media organisations, think tanks, academics and journalists

- 13 countries largely in central and eastern Europe have already signed up for assistance.

These details are precisely as described in the documents leaked in March 2019. There are solid grounds to consider them authentic.

EXPOSE Network Proposed by the CDMD

An undated draft proposal from the Foreign and Commonwealth Office (FCO) stated that the network (subsequently identified as EXPOSE) is part of the CDMD program headed by Andy Pryce. It is inconceivable that he didn't at least authorise this draft. The proposed contract creates the role of a Network Facilitator to run the Network Hub of the EXPOSE network.



DRAFT

Terms of Reference for contractors to develop a network of NGOs exposing disinformation

INTRODUCTION

The Foreign and Commonwealth Office is looking for a consortium of contractors to build a network of actors who expose disinformation across Europe, provide core funding to NGOs with the most potential for impact and build the legal/ethical, tradecraft, communications and security capacity of these organisations.

OBJECTIVE

This project is part of the FCO's Counter Disinformation and Media Development (CDMD) Programme, which implements new and innovative projects to counter disinformation and propaganda. The CDMD programme seeks to build media plurality in Northern and Eastern Europe, engage with populations groups vulnerable to disinformation, expose disinformation in a variety of ways and to monitor and understand disinformation activity and its impact.

The overall objective for this project is to expose malign state disinformation in European countries that are targeted by it.

A scoping study has identified 56 different organisations from Georgia to Spain who research, identify and expose state disinformation activity in a variety of ways.

1. **Project Scope**

It is anticipated that the project will work will be conducted across European Union and Easteen Partnership countries.

Project recipients will be non-governmental organisations.

The winning consortia will be expected to

- Deliver outcomes to part of a theory of change specified by the FCO
- Develop a results framework and risk management strategy for their work
- Conduct due diligence on each of the 56 potential network members
- Assess the training needs of each organisation
- Deliver tailored capacity building on legal/ethical issues, open source information gathering, communications/pr and physical and personnel security to organisations in the network
- Provide targeted core support where it is likely to achieve the strongest possible outcomes
- Bring the diverse collection or organisations together as a network to increase their mutual understanding of disinformation activity, allow them to share information and to more thoroughly expose and frame hostile state activity.
- Ensure the outputs of the network is used by a wide range of media outlets as possible and gains prominence on social media

As later stated by Haynes, this document confirms the draft of a £10 million contract over three years, with an anticipated roll out in the summer of 2018. The successful contractor is asked to *'assume'* independence. In light of the level of direct CDMD control built into the contract, this *'assumption'* appears to be little more than coded language for maintaining plausible deniability. It also identifies the EXPOSE Network as a priority for the CDMD.

The proposed contract creates tight reporting and monitoring procedures for the Network Facilitator (Zinc consortium) to report directly to the FCO and their stakeholders (monthly, quarterly, ad-hoc). It proposes the FCO (CDMD) veto over the project's activities and evidences the CDMD's control of the EXPOSE Network is *hands on*. The FCO also request that the operation be *'overt'* and no attempt made to *'hide activity.'* Again, this seems disingenuous. All associated with the

EXPOSE network are required to sign strict non disclosure agreements (NDA's), hiding their activity.

The CDMD were seeking to create a network Hub to build (fund, train and equip) a European wide network of actors in tradecraft, security, capacity and greater communication impact. In Northern and Eastern Europe the CDMD wished this *'network of actors'* to engage with groups *vulnerable to disinformation* (people who question official narratives) to expose (attack) and monitor (report) claimed disinformation back to them.

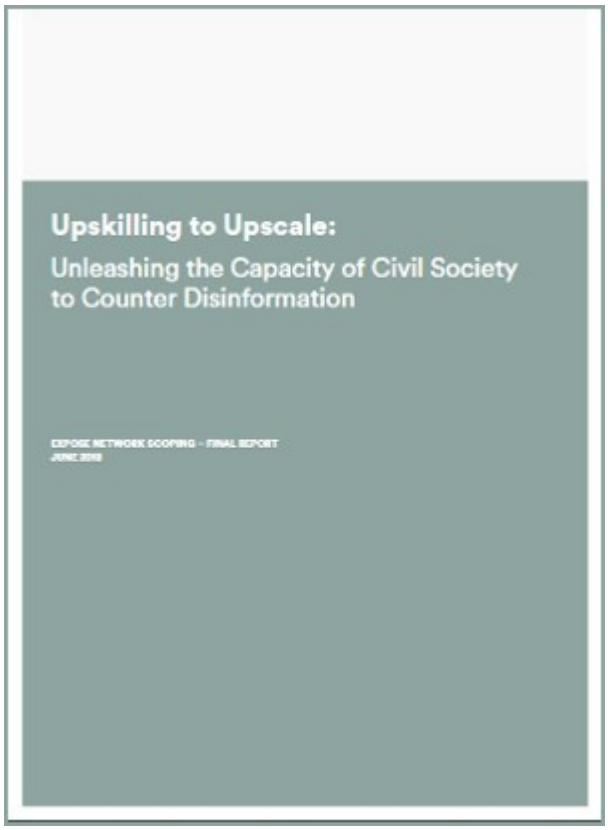
This is the first indication that the EXPOSE network is a joint UK EU initiative. Given that the UK were supposedly intent upon leaving the EU, the fact that they were planning a cooperative project with the EU in 2018 is notable.

The proposal shows the operation was planned to be conducted across the EU and Eastern Partnership and that 56 potential network partners had already been identified. To imagine this could be done without the EU's full knowledge and consent is untenable. As we shall see, the EXPOSE Network is part of a much wider EU/NATO/UK counter disinformation effort.

The successful contract bidder needed to have experience of open source intelligence (OSINT) gathering. They had to demonstrate the capacity for securely handling sensitive information with government partners. The supplier was asked to create a *'secretariat'* to report development and outcomes to the CDMD and their partners. They also needed to demonstrate their ability to work under direct instruction of the CDMD to target 'ad-hoc' *tactical opportunity.*

EXPOSE Network Takes Shape

The document Upskilling and Upscale: Unleashing the Capacity of Civil Society To Counter Disinformation is dated June 2018 and is the EXPOSE Network's final scoping report. It fleshes out the details of the framework suggested in the CDMD's draft contract proposal.



Andy Pryce apparently attended a workshop discussing a network of NGO's on Wednesday 8th of August 2018 where he gave feedback on the terms of the contract. Zinc Network submitted their consortium bid to the FCO in a technical proposal dated 31st August 2018. So it seems likely that interested parties gathered to discuss the creation of the EXPOSE Network around late July to early

August 2018.

Upskilling and Upscale gives a clear insight into the operation of the EXPOSE Network. It states:

"The EXPOSE Network sets out to identify civil society organisations (CSO) operating across Europe countering disinformation using a variety of tactics, upskill these organisations in research and communications and through the provision operational support, grants and training, and coordinate their activities to ensure effectiveness and measure impact through research and evaluation.....If supported to deliver their activities in a professional manner that holds them above reproach.....these organisations have the potential to be the next generation of activists in the fight against Kremlin disinformation."

The document makes it clear that everything which challenges western state narratives is *Kremlin disinformation*. At no stage are the EXPOSE partners asked to consider the evidence substantiating this claim. It is stated as fact without evidence. The potential network actors included Bulgaria Analytica (Bulgaria), Istinomer (Serbia), Global Focus (Romania), Euroradio (Belarus), Grass Factcheck (Georgia), the Institute of Public Affairs (Poland), Sut.Am (Armenia), the Prague Security Studies Institute (Czech Republic), Bellingcat (UK), Factmata (UK) and the Institute for Strategic Dialogue (UK).

With the exception of Bellingcat, there is no evidence that any of these organisations, or others listed in the document, are currently directly involved in the EXPOSE network. However, it is likely some are.

In Part 4 we'll start to look in more detail at the network of CSO's, NGO's, governments and multinational corporations behind the EXPOSE network.

However, if we just look at Serbia's Istinomer they are funded by, among others, the EU, USAID (U.S State Department), the National Endowment for Democracy (U.S intelligence agencies), Google, Microsoft, The Rockefeller Foundation and the Canadian, Norwegian, Dutch & Swedish governments. One of their listed partner organisation is the Westminster Foundation for Democracy (WFD), a UK parliamentary body sponsored by the Foreign and Commonwealth Office. In turn, the WFD's listed partners are the World Bank, the EU, the United Nations Development Program (UNDP) and the Organisation for Security and Cooperation in Europe (OSCE).

While we cannot categorically state, at this stage, that Isinomer are network actors for the EXPOSE network, they represent a typical example of the organisation suggested in the scoping document. Their extensive international network of powerful backers are also common to the groups named.

Research Underpinning the EXPOSE Network

The scoping research for the EXPOSE network was carried out by media outlets, think tanks, and grassroots implementers running projects that included promoting media literacy and community cohesion. They found that, despite significant claimed achievements in the fields of fact-checking and debunking, there were core weaknesses in research, public facing campaigns, network analysis, investigative journalism and media literacy.

In other words, the FCO's research discovered their desired message wasn't getting through. People just didn't believe their narratives in sufficient numbers. Therefore, as it is deemed impossible that official accounts, such as the highly implausible Skripal poisoning yarn, are anything other than the purest form of truth, these failing must be due to *Kremlin disinformation*.

The lack of evidence, or contradictory evidence, undermining official western state versions of events is never broached. All communication breakdowns are the Kremlin's fault.

Everyone who questions the policies, announcements and actions of EU/NATO aligned states are identified, by the EXPOSE network, as either willing or unwitting agents, assets, trolls or bots of the Kremlin. This includes, but isn't necessarily limited to, whoever the state decides is a far right or a far left group (no definition); people they consider anti-Zionists (no definition); anyone they label a conspiracy theorist (no definition); people who don't hate the Russian's, or *"Kremlin sympathisers"* as the FCO put it (no definition); those who criticise the mainstream media (I think that's just about everybody), fringe networks (no definition) and, even worse, fringe networks who share content using mainstream hashtags, resulting in unwanted information *"bleeding into the mainstream."* Twitter users basically.

The FCO go on to identify four reasons why *Kremlin disinformation* has been so successful. Reading their findings does beg the question how much this scoping research cost. They appear to have uncovered little more than the glaringly obvious.

The first *'reason'* was that it speaks to people who already disagree with the government. There's no acknowledgment that people have the right to disagree with the state and may do so for their own reasons, without Kremlin influence. Anti war protestors are invariably critical of government policy. They don't all work for the Kremlin.

The FCO researchers then discovered the Internet and the existence of modern communication technology. They realised this meant ordinary people could spread *disinformation* via their blogs, videos, social media posts and memes. Therefore they suggested the need for more censorship to stop the opinionated circumnavigating a *"weak regulatory environment."* The final identified reason was that people haven't been properly programmed to accept the right information from the right sources and need educating in *'critical media consumption.'*

Who Checks The Fact Checkers

The EXPOSE Network extends across Europe and parts of Central Eurasia. The specific regions for the OIP to target are the Balkans, the Baltics, Central Europe, the Caucasus, Eastern Europe, Southern Europe and Western Europe (including the UK).

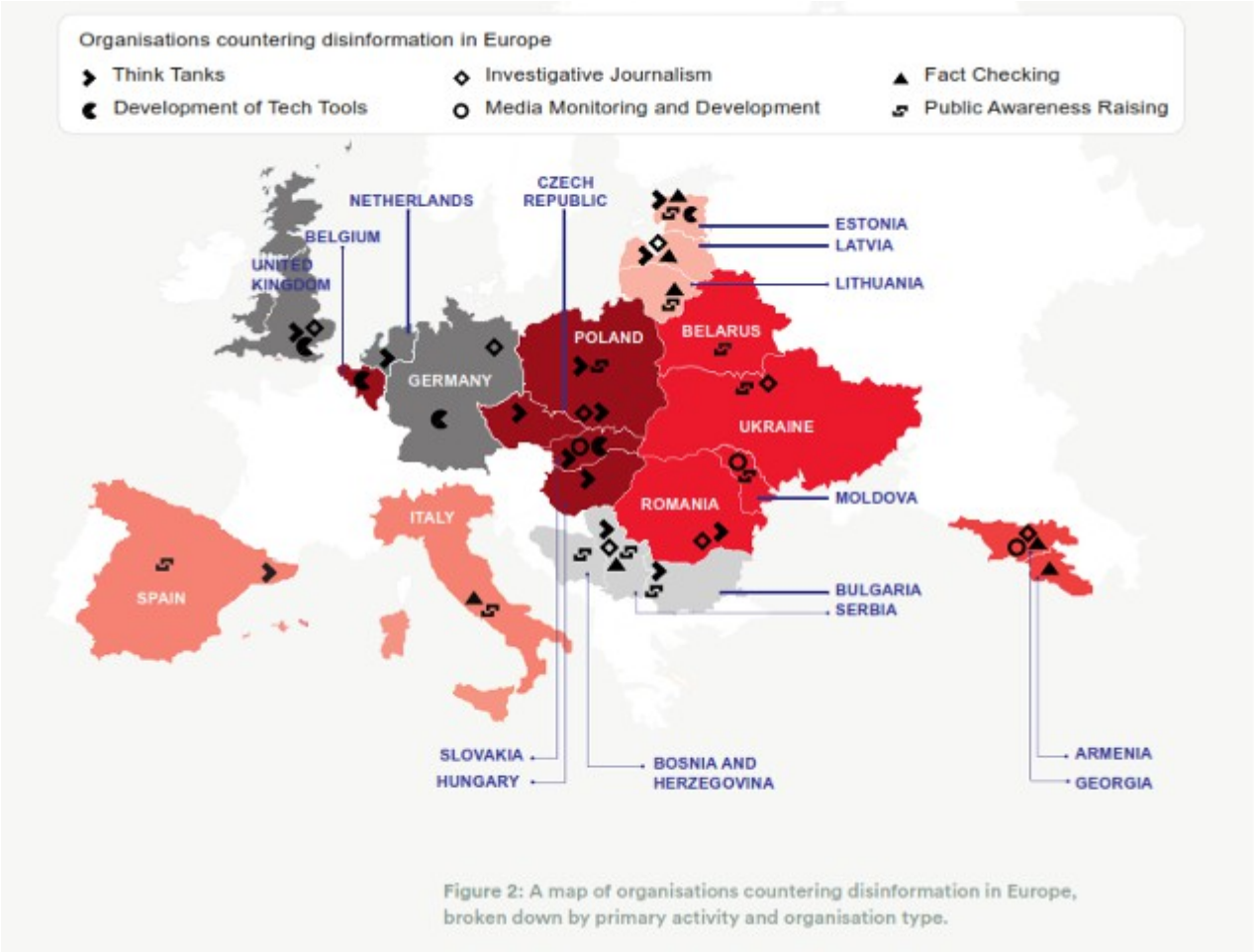


Figure 2: A map of organisations countering disinformation in Europe, broken down by primary activity and organisation type.

The relative effectiveness of four key strategies for combating *Kremlin Disinformation* were analysed. Fact checking and debunking aimed at *"stopping journalists and amplifiers from sharing disinformation content,"* was deemed effective; the painstaking research required for investigative journalism was considered too slow (unable to respond in real time) so monitoring social media using online tools was advocated instead; public campaigns targeting "*groups susceptible to kremlin disinformation*" (see above) were also looked upon favourably.

International Fact Checking Network

The FCO suggested their network of actors either use approved fact checking services or develop in house capability based upon the Poynter fact checking principles. These are the principles which all members of Poynter's International Fact Checking Network (IFCN) must adhere to. Poynter's major funders include the Charles Koch Foundation, the National Endowment for Democracy (NED), the Omidyar Network (Luminate), Google and the Open Society Foundation.

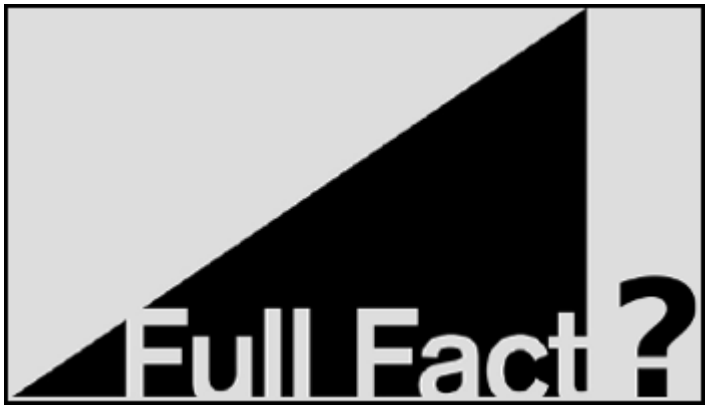
Poynter were forced to issue an apology to a number of media organisations in May 2019 after they issued an index of *'unreliable'* media sources. When some listed organisations inquired about the basis for Poynter's declaration, requesting Poynter provide some evidence to back up their claims, Poynter quickly removed the suggested *"blacklist."*

Poynter's IFCN make a great deal out of their fact checking principles so it's a shame they didn't apply any when they issued their blacklist. Poynter's managing editor, Barbara Allen, said the purpose of the blacklist *"was to provide a useful tool for readers to gauge the legitimacy of the information they were consuming."* Continuing Poynter's apology, she added:

"We began an audit to test the accuracy and veracity of the list, and while we feel that many of the sites did have a track record of publishing unreliable information, our review found weaknesses in the methodology. We detected inconsistencies between the findings of the original databases that were the sources for the list and our own rendering of the final report."

This was tantamount to Poynter admitting they chose who to put on the potential blacklist based upon their *feelings* towards them. When requested to evidence their decision they couldn't.

The fact checkers, who are signatories of the IFCN code, include Politifact, Snopes, Full Fact, StopFake and AP Fact Check, to name but a few. Taking just Full Fact, as an example, their corporate members include the City of London Corporation (the UK financial sector and a global center for international finance), the global corporate law firm King & Wood Malleson, St Jame's Place Wealth Management, a huge global capital investment firm, and the defence contractor Rolls Royce. FullFact's individual donors include Google, the Omidyar Network and the Open Society Foundation. They are also supported by the UK Government's Office for National Statistics (ONS).



Do all of these global corporations, wealthy foundations and government agencies care passionately about people getting their facts straight? Certainly Facebook

believe so, as FullFact has been one of their fact checking partners for some time. Their role being to assist the social media platform to *'down rank'* allegedly *'debunked'* articles and posts. Thereby, keeping the exchange of information to an absolute minimum.

When we look at the IFCN and their fact checking signatories, it is clear that they are backed by powerful globalist interests. There is absolutely no reason at all to imagine any are remotely objective.

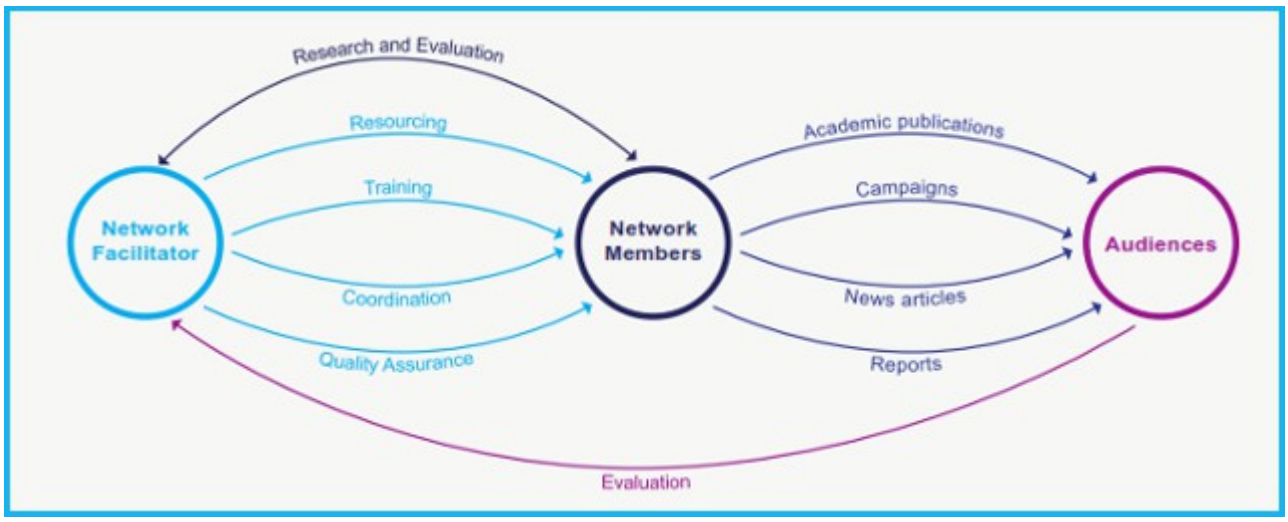
The EXPOSE Network, having encouraged their network of actors to subscribe to the U.S. based Poynter IFCN fact checking principles, don't recommend they observe the U.S. based Society of Professional Journalists (SPJ) code of ethics. The SPJ ethics code demands that journalists:

"Recognize a special obligation to serve as watchdogs over public affairs and government. Seek to ensure that the public's business is conducted in the open, and that public records are open to all."

and….

"Be vigilant and courageous about holding those with power accountable. Give voice to the voiceless."

The CDMD opted for their network of actors to adopt the NUJ code of conduct. Unsurprisingly, this has nothing at all to say about speaking truth to power.



The EXPOSE Network

The Fourth Way – Network Analysis

We have already discussed the EXPOSE Networks first three approaches to countering disinformation and their suggested reliance upon the right fact checkers. It is perhaps their fourth strategy of network analysis that reveals most about their intentions. NATO's Atlantic Council's Digital Forensic Labs (DFRLabs), also resource members of the Open Information Partnership, are highlighted throughout as exemplary. Referencing them again, as leading exponents of network analysis and mapping, the CDMD state:

"This mapping is key to both understanding the emerging field and for designing interventions. Exposing networks of sources that spread disinformation, rather than trying to counter specific stories and pieces of content, may be one of the most effective and sustainable ways of countering disinformation. Highlighting sources which people have previously trusted and showing that they are attempting to malignly influence the conversation can activate a sense of being manipulated and act as an affront to an individual's deeper emotional and psychological need to see themselves as rational and informed. For example, the Kremlin repurposed

bot/ troll accounts and exploited the same far left and far right communities for both the anti-White Helmets and pro-Brexit campaigns in the UK. Exposing this finite network of disinformation nodes can have a long term counter disinformation impact."

It is clear the EXPOSE Network's actors, rather than offer evidence which supports their narratives, are encouraged to *'expose networks of sources.'* Their task is to *undermine* those who disagree with EU/NATO *'facts.'* They will be taught how to use *'emotional and psychological'* techniques to target *'this finite network of disinformation nodes.'* Shoot the messenger is the EXPOSE Network mantra.

Excellent and trustworthy sources of 'evidence.'

There is a wealth of evidence that the White Helmets are a UK state run propaganda and intelligence operation created in Turkey by a former British intelligence officer. Whether the interpretation of those facts are accurate or not, they exist. The network analysis and mapping, operated by the EXPOSE network, is designed to deny those facts. Not by debating them or offering counter

evidence, but simply by labeling those reporting the facts as *Kremlin disinformation* agents.

However, it is the identification of *pro-Brexit campaigns* in the UK which should perhaps prompt the greatest concern. Quite obviously the EXPOSE Network is an overtly political organisation. The pro EU/NATO agenda is its founding precept. Everything it does is in support of EU and NATO objectives and the foreign policies of the government's who share them. We have touched upon the network of western aligned globalist institutions who are deeply involved in the EXPOSE Network. They too have vested interests in maintaining and promoting EU/NATO foreign policy objectives.

The EXPOSE network has been created as part of a transatlantic effort to police information in the Internet age. By combining with proposed legislation, the tech giants and approved fact checkers, the aim is to transform both the Internet itself, and the information environment, in order to re-engineer state control of ordinary citizens access to verifiable facts.

Redefining Journalism

The EXPOSE Network's attempt to redefine investigative journalism. Their new definition has nothing to do with questioning power and suggests journalism is at its best when it is monitored and controlled by the state:

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

narrative television and other accessible formats…….Journalists and mainstream media outlets; through embedded investigative journalism projects and the mapping of networks and sources, network members will provide facts to journalists and mainstream media outlets that prevent falsehoods reaching the mainstream media……The ongoing monitoring and evaluation will provide a comprehensive picture of activities happening across Europe and their impact on a micro and macro level, and will give the FCO the ability to coordinate activity in response to specific events or narratives being spread by Kremlin-backed media"

Given the evidence we've looked at thus far we can paraphrase these statements. Embedded state controlled journalists, within mainstream media organisations, will receive information from the Expose Network and then report the facts provided to them by their state controlled fact checkers. These are predetermined to establish links with *'far right movements'* such as the *'pro-Brexit campaigns in the UK.'* The embedded mainstream media journalists will then use the EXPOSE Network's *'mapping of networks'* to run counter disinformation media campaigns against anyone who criticises EU/NATO aligned policy. Making sure information never sees the light of day on an MSM dominated and tightly restricted Internet.

The threat posed to our supposed democracy by the EXPOSE Network is immense. It has absolutely no intention of promoting independent, evidence based investigative journalism. It's pretensions of *counter-disinformation* are nothing but a thin veneer for a comprehensive European propaganda network. Claims of encouraging *critical thinking* are a travesty. It is concerned only with the absolute control of information, denying the public even the faintest opportunity to explore evidence the state doesn't want them to see.

In the next chapter we'll look at the evidence which demonstrates how the EXPOSE Network facilitator operates.

Chapter 4: The Role of the EXPOSE Network Facilitator

In June 2018, the Foreign and Commonwealth Office's (FCO) Counter Disinformation and Media Development (CDMD) program issued their final scoping report for the the proposed EXPOSE Network. It established the role of a Network Facilitator to act as the central coordinator for the EXPOSE network of civil society organisations (CSO), non governmental organisations (NGO), fact checkers, smaller civil activists groups, journalists and bloggers across Europe and parts of Central Eurasia. The Network Facilitator would operate out of the Network Hub from where they could provide the technical & legal support, cyber & physical security, funding and training for the *network of actors*.

In the scoping report the FCO recommended that the Network Hub be based in a secure central European city, for logistical ease as much as security. The EXPOSE network was also designed to act as a European online listening station reporting claimed *Kremlin disinformation,* which appears to be anything that disagrees with EU/NATO policy, back to the UK CDMD and FCO. Outlining the Facilitators role, the scoping report stated:

"The Network Facilitator will provide a centralised social listening function and media monitoring, tracking key disinformation narratives across Europe…….In turn, organisations will be provided with access to the latest social listening tools and training in how to use them……..including mapping the sources and networks of these narratives and the audiences that are the most vulnerable to them……..This information can then be shared with the FCO, via the Network Facilitator ensuring that all data is gathered……"

The EXPOSE Network Facilitator

The Network Facilitator contract was won by a consortium led by Zinc Network. They submitted their technical proposal on or after the 31st August 2019. We know this convinced the FCO to offer the Zinc consortium the contract. As with most contract bids, the FCO CDMD would have been interested to see what *'added value'* Zinc could offer them. We cannot be certain which elements of that added value the CDMD, who maintain close control of the EXPOSE Network, chose to adopt. We can be more confident about the elements of the Zinc consortium are contractually obliged to deliver. These were specified in the scoping document and broadly outlined in the draft proposal.

The resource partners of the Zinc consortium are Bellincat, the Atlantic Council's DFRLab and the Media Diversity institute. The main implementing consortium partners are the Institute of Statecraft and Aktis Strategy. Zinc Network are both resource and implementing partners. The consortium's risk and security partner is said to be Toro Risk Solutions and the financial management of the Hub's grant system is reportedly provided by Ecorys.

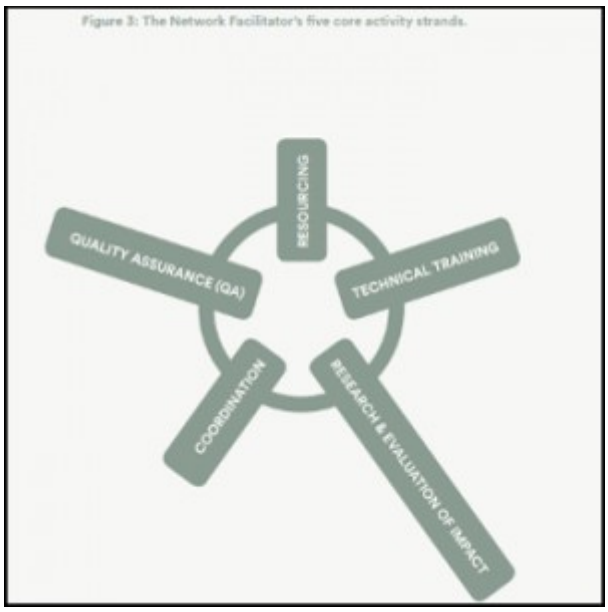
Zinc, Bellingcat, DFRLabs and the Media Diversity institute are the listed resource partners on the OIP website. There is further evidence that the Institute of Statecraft (in some form) and Toro Risk Solutions remain involved. However, the current status of the Institute of Statecraft is something we'll discuss in Part 4. The role of Ecorys as possible grant managers is consistent with information released. Aktis Strategy, as a company, are definitely no longer involved, though former employees may be.

The Zinc Consortium Delivers

Anyone who reads the Zinc consortium's (ZC) technical proposal can either see it as a perfectly legitimate and necessary addition to the UK's national security effort or utterly horrifying, depending upon their beliefs. For all the reason we have previously covered, personally I find it chilling.

ZC state:

"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."



The Network Hub is the Open Information Partnership, currently represented by nothing more than single page website. The webpage is essentially a ruse (disinformation) to sell the idea that the OIP is a public, open and transparent organisation. It meets the FCO's request that the operation be *'overt'* and no effort be made to hide it. Like their suggestion that the Network Facilitator *'assume'* autonomy, this looks like an attempt by the FCO to maintain *"plausible deniability"*. Noting this desire, ZC remark:

"*To be sustainable and less vulnerable to attack from malign actors, the Network needs to be public-facing…… the strategy for public facing communications is based on minimum requirements, such as a static website……..The project could expand to build on this public facing component, promoting the network as a journalist integrity and disinformation network……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.*

Nowhere on the OIP single page website does it make any mention of the *discrete* nature of the wider network's activities. Reputational management seems the sole reason for the webpage's existence.

There is little doubt about the clandestine nature and precarious morality of the EXPOSE Network, openly addressed in numerous documents. In a bid to win the contract, ZC gave assurances to the FCO that their reputation would be protected:

"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 (the FCO CDMD)."

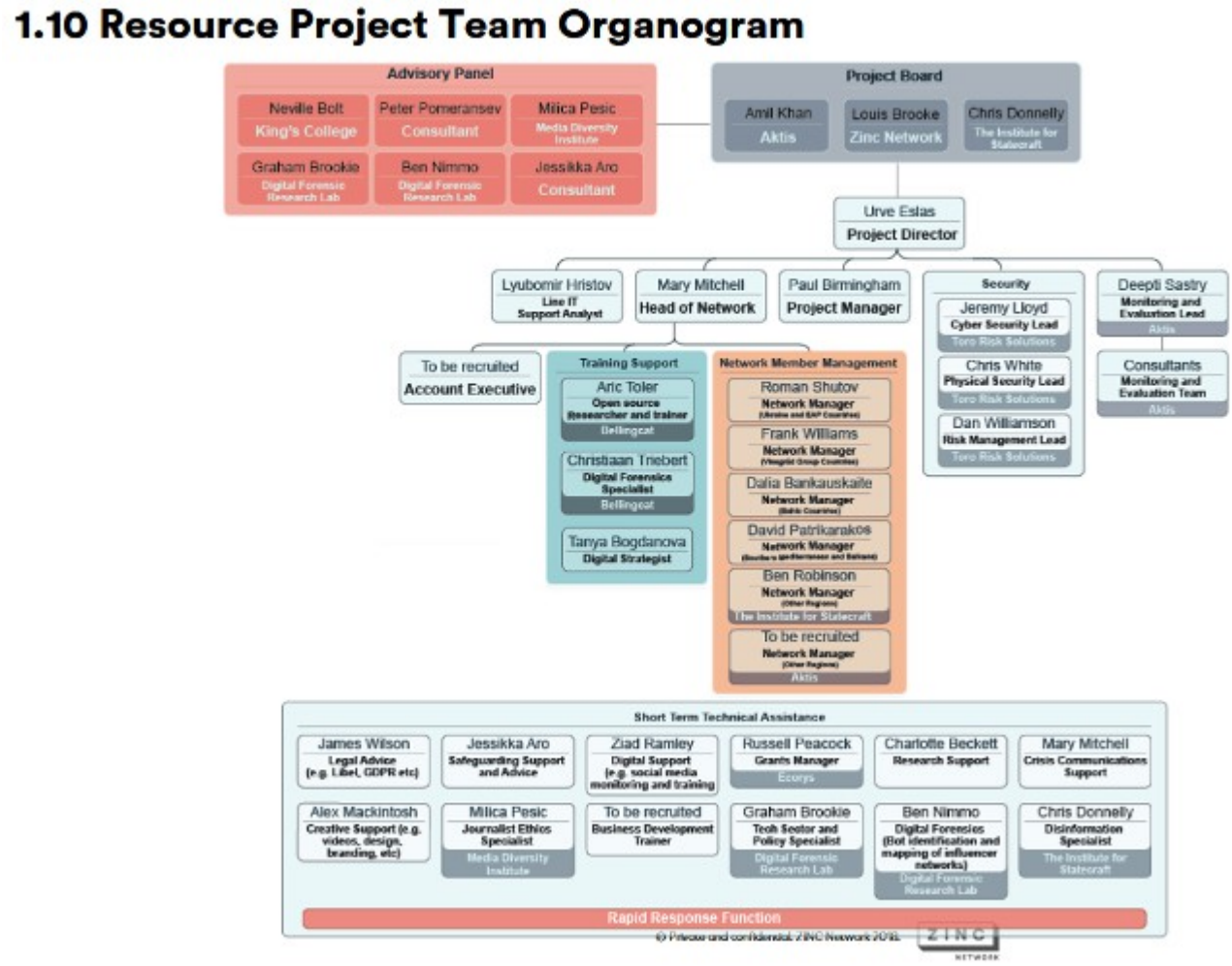
[Note: Bracketed information added.]

ZC had good reason to manage risk in this way. They, or rather the people they train and support who form the '*network of actors*,' are put in potential danger. The technical proposal is complete with case studies which reveal the ZC's capabilities and experience of managing these risks:

"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…….. and carefully managing project communications to keep their involvement confidential."

Whatever you may think of the EXPOSE Network, while many names of those

within the *network of actors* are now in the public domain, only those already identified as being part of the Network Facilitator, EXPOSE Network and the Open Information Partnership are identified in this series.



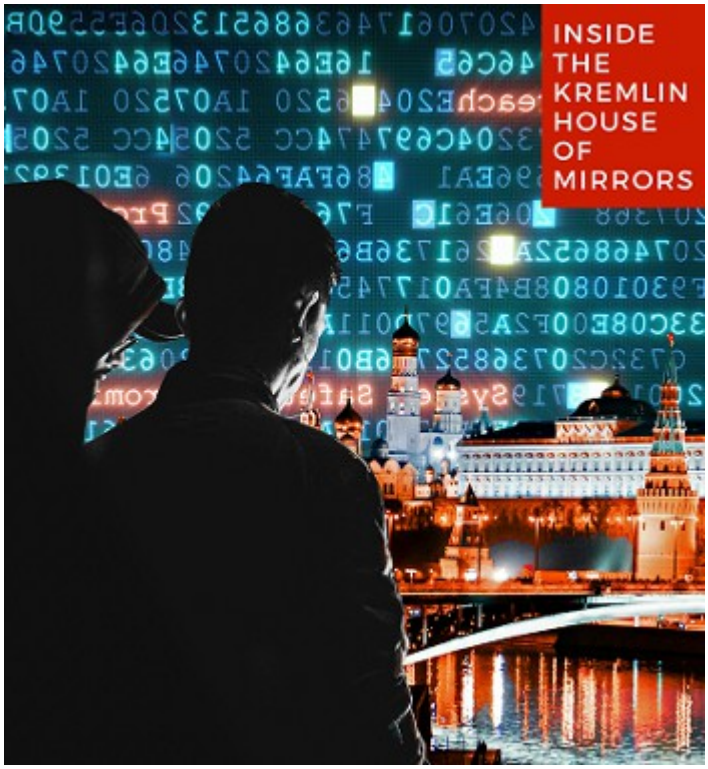
The Network Facilitator within the OIP

Zinc Consortium Are Watching You

As previously discussed, the purpose of the EXPOSE Network (hence the name) is to seek and identify those who are deemed to be peddling *Kremlin disinformation*. This essentially boils down to anyone who questions EU/NATO policies,

narratives, actions or objectives. For example, Pro Brexit campaigners are cited as an *'audience vulnerable to disinformation.'* The ZC spell out their strategy for dealing with such people. Their network of actors will be trained by ZC's in-house digital experts:

".....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."



Kremlin Disinformation – Everyone's doing it

If this all sounds rather familiar it is because this activity is precisely the allegation leveled against the Kremlin by western states and the mainstream media. In seeking to defeat what they claim is *Kremlin disinformation,* the EXPOSE network is deploying the same operation they insist they are fighting

against. Chicken and egg springs to mind.

ZC state they will:

"*…..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."*

As discussed in Part 2 none of these terms are clearly defined. Policy makers for instance could be anyone from elected politicians to committee members, advisers or think tank participants.

The ZC go further. They advocate targeting individuals and deploying behavioural change techniques. Alluding to the Behavioral Insights Team (BIT), the UK Government's former in house *'Nudge Unit,'* repurposed as a commercial enterprise in 2014, the ZC suggest applying psychological manipulation to change thinking.

"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…….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"

The ZC were careful to couch this suggestion in terms of inviting individuals to join their counter disinformation effort. However, in the wider context of the EXPOSE Network's obvious purpose, the implications are clear. The ZC were highlighting their capability to target *concerned citizens*.

We acknowledged in Part 1 that Russia run propaganda and disinformation campaigns. All developed nations do. However, there is no evidence that they are operating on anything like the scale of the EXPOSE Network. The strongest evidence released so far seems to show some very basic and largely ineffectual online adverting campaigns.

Whoever is labeled as a *Kremlin disinformation* agent, asset, troll or bot will then be reported by the ZC back to their FCO handlers in real time:

"Clear and consistent client reporting (to the CDMD) is essential to maintaining a

strong and productive relationship with the FCO……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.…"

[Note: Bracketed information added.]

Using the raft of Internet *'safety'* legislation currently being rolled out, EXPOSE Network *'supporters'* like Google, Facebook, Twitter and others, can then be directed to purge the offending accounts. Along with the information, including any evidence, they direct the public towards. The Internet, as we know it, is increasingly being controlled. Access to information will be limited by the state and their corporate partners.

The EXPOSE Network Rapid Response

Speaking in June 2018, following the G7 summit, then UK Prime Minister Theresa May announced the G7's Rapid Response Mechanism. The G7 stated that hostile state activity will be met with a rapid and unified response. Alleged hostile states will be identified for their *'egregious behaviour'* and there will be swift, coordinated international attribution of guilt for cyber and other attacks.

Effectively they were declaring that foreign states will be blamed immediately for any event the G7 claims they are guilty of. No evidence or investigation required. Just arbitrary ascription of blame and rapid retribution. Apparently, this dangerous lunacy is part of the laboriously advocated *'international rules based system.'* It appears to differ somewhat from International Law which focuses more upon concepts shunned by the G7, such as due process and evidence.

The G7: Able to respond rapidly to whatever they like

Earlier, in January 2018, the UK Government announced the creation of the National Security Communications Team (NSCT). This team of civil servants advise the Cabinet and Prime Ministers Office. Headed by Daniel Walpole, their role is to assist the UK Government with communications challenges related to national security, including (but not limited to) disinformation. In April 2018 they were joined by the Rapid Response Unit (RRU) who, in times of crisis, work closely with the NSCT.

The RRU monitors digital trends to spot emerging issues, including misinformation and disinformation, and identifies ways to respond. The Director of Government Communications Alex Aitken, speaking about the RRU, stated:

"Following the Syria airstrikes, the unit identified that a number of false narratives

from alternative news sources were gaining traction online. These "alt-news" sources are biased and rely on sensationalism rather than facts to pique readers' interest. Due to the way that search engine algorithms work, when people searched for information on the strikes, these unreliable sources were appearing above official UK government information…….The unit therefore ensured those using search terms that indicated bias – such as 'false flag' – were presented with factual information on the UK's response. The RRU improved the ranking from below 200 to number 1 within a matter of hours"

The claim that only *official UK Government information* is factual and unbiased is both notable and demonstrably false. Yet it is Aitkens other claims about RRU/NSCT capability which are perhaps more interesting.

Don't worry. Everything is under control.

The process of Search Engine Optimisation (SEO) is a technique for creating content which ranks well for specific search or keywords. This involves *'optimising'* for a whole range of *'metrics'* which form the Google organic search algorithm (predominantly). An allegedly closely guarded secret, cracking the Google organic search algorithm is the holy grail for marketing companies the world over.

Even the WPP Group would struggle to take a web page's organic Google search ranking from below 200 to number 1 in a few hours. What Aitken appears to reveal here is that the UK Government work with Google to fix the search results. Not so much a search engine, more of an official government statement website.

Google are prominent supporting partners of an array of EXPOSE Network partner organisations (see Part 4 and Part 5).

Advocating their *Rapid Response vehicle* the ZC offer the Counter Disinformation and Media Development Program the following service:

"….by coordinating members' (network of actors) 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…….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."

[Note: Bracketed information added.]

A recent report by the internet market researchers SearchMetrics looked at how Google ranked a range of Brexit related Keywords. They clearly showed the overwhelming dominance of the UK state broadcaster, the staunchly pro EU BBC, in the search results, closely followed by the other mainstream media outlets. The BBC are tasked with propagating official government announcements. The BBC charter states the 'public purpose' of the BBC:

"To reflect the United Kingdom, its culture and values to the world: the BBC should provide high-quality news coverage to international audiences, firmly based on British values of accuracy, impartiality, and fairness. Its international services should put the United Kingdom in a world context, aiding understanding of the United Kingdom as a whole"

The BBC is publicly funded by license payers and that fee is controlled by government legislation (2003 Communications Act). Their funding settlement is set by the UK Secretary of State. Like the EXPOSE network, they are a UK government department in all but name.

Seeing as the UK government appear to be in partnership with Google, who dominate the Internet search market, the BBC's near monopoly of search results related to contentious political issues isn't surprising. It is now possible to envisage how the Rapid Response Mechanism will work from the public's perspective.

The G7 will blame another country for some event or crisis. Claims of cyber attacks, the evidence for which is *'virtual'*, are extremely vulnerable to state manipulation. Currently it appear most likely that either Russia, Iran or China will be blamed should a cyber attack occur. However, it could be any foreign power that falls into the G7's cross-hairs. Yemen maybe? Blame will be attributed without any investigation or any need of proof. Evidence is irrelevant.

This will be accompanied by a slew of '*counter disinformation'* content pumped out by the EXPOSE Network. They will also rapidly identify anyone who questions the G7's assertion. The '*counter disinformation'*, accurate or otherwise, will support the G7 narrative without question.

Governmental communication strategists in groups like the UK's NSCT and RRU will then work in partnership with the major search engines, MSM outlets and social media partners to ensure the G7 message is ubiquitous across all platforms. Elevating EXPOSE content and other *approved* information via a network of *'embedded'* journalists and MSM assets. Meanwhile, based upon information received from the EXPOSE Network, any dissenting voices asking questions or advocating restraint will be *'down graded'* and relegated to relative information obscurity.

It appears that dissent will not be tolerated.

The EXPOSE Networks Proposed Election Strategy

The recent Mueller Report, in the U.S, into alleged Russian *'hacking'* of the 2016 election failed to produce any substantial indictable evidence to prove the allegations of Russian interference, or state collusion. A small team of Russian trolls on social media is hardly a threat when faced with the magnitude of an operation like the EXPOSE Network.

The plot doesn't thicken.

We don't know if the FCO CDMD authorised the *'added value'* offered by the ZC, only that they offered them the contract. However, if they did, then clearly meddling in elections is firmly on the EXPOSE Network's agenda:

"Elections are often a flashpoint for disinformation ……the Network could focus project resource on elections taking place in countries that are of particular interest to the FCO. The Network would…..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…….. The team could test different approaches to engage targeted audiences through mainstream media or governments……..We could also work with social media providers……We could also build some Network Members into a longer-term election cluster of organisations who prioritise this in their routine activity."

It is difficult to imagine how a propaganda operation of such ambition could

possibly deliver on a budget of £10 million over three years. Of course it can't and were its budget truly £10 million it wouldn't. However, potentially available government funding is far in excess of this amount. The CDMD is funded by the UK Conflict Stability and Security Fund (CSSF). They alone have an annual budget of £1.3 billion. Yet there is far more European state funding than that on the table. We discuss this in Chapter 7.

It isn't just governments who are attracted to the EXPOSE Network either. Adding further value to their bid, the ZC stated:

"Zinc will also encourage other donors to provide additional financial resources to the Network and the wider sector."

The EXPOSE Network's listed partner organisation are collectively funded by a huge international network of governments, NGO's, philanthropic foundations, wealthy individuals and multinational corporations. Acting collectively in support of the EXPOSE Network, available resources are feasibly limitless.

It is this interconnected web that we'll begin to explore in the next chapter.

Chapter 5: The EXPOSE Network's Partners

We are going to start to explore the web of interconnected NGO's, CSO's, governments, intelligence agencies and multinational corporations behind the EXPOSE Network. This enables the potential budget and resources for the network to increase, practically without limit.

When the former Minister of State and member of the Parliamentary Intelligence and Security Committee Alan Duncan announced the Open Information Partnership (OIP), he made reference the potential for the EXPOSE Network to expand its funding sources:

"We have a regular dialogue with international partners on the challenge posed by hostile state disinformation, including to align donor support in this field."

"Donor support" comes from the substructure of organisations, both governmental

and non governmental, who use various NGO's, charities and foundations as funding vehicles to *'support'* causes favourable to their business and/or political objectives. Their philanthropy and charitable giving is always promoted as humanitarian, depicting wealthy donors and government agencies as caring, global custodians.

However, even the most cursory research soon makes it abundantly clear, in the vast majority of cases, multinational corporations, and those who own them, don't invest their money in anything unless it serves their interests. These rarely align with the people's, but they do frequently coalesce with government policy shaped by the same corporations through a multi-billions dollar lobbying industry.

In their technical proposal to the UK Government Foreign and Commonwealth Office (FCO), Zinc Network clearly outlined how they could bring in plenty of *"donor support:"*

"Zinc 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."

Whether this convinced the FCO to offer the Zinc consortium the contract isn't clear. Having NATO on board, in the shape of DFRLab, was probably viewed as encouraging by the FCO. It certainly wouldn't have harmed their bid. The scope and ambition of the EXPOSE Network propaganda operation quite obviously costs considerably more than the officially allotted £10 million over three years. The money has got to come from somewhere.

The EXPOSE Network resource partners are Zinc, Bellingcat, DFRLabs and the Media Diversity Institute. The main implementing consortium partners are Zinc, the Institute for Statecraft (in some form) and Aktis Strategy (bankrupt). Risk management is reportedly provided by Toro Risk Solutions and Ecorys are said to be the financial managers of the grant fund.

Aktis Strategy no longer exist though some of their former personnel may still be involved in the project. The Institute of Statecraft's current status is difficult to ascertain but there is a high likelihood that they, or their former team members, remain involved in some capacity. While we cannot categorically state that Toro Risk Solutions are still part of the EXPOSE Network, if not them, then a similar organisation capable of delivering the same level of security are. The same can be said for Ecorys.

Therefore, we are going to focus upon DFRLabs and the Media Diversity Institute here. We'll look at Zinc & Bellingcat in the next post . These four are the listed resource partners on the solitary OIP webpage. When we look at the access they have to '*resources,*' the name fits. Before that, let's first take a quick look at the other likely consortium members.

Aktis Strategy

Blaming poor financial management and cash flow problems Aktis Strategy declared bankruptcy on 14th March 2019. Formed in 2013, Aktis rose incredibly quickly to become a leading contractor for the UK Government. Primarily for the FCO and the Department for International Development (DfID). They worked on security and development programs in countries including Iraq, Tunisia, Syria, Turkey, Somalia, and Lebanon.

Aktis Strategy's sudden demise potentially left many projects in crisis. There were significant concerns about this and the loss of financial data. This was a worry

expressed in Somaliland, for example, where Aktis were worked with another British company Axiom International. Aktis' Twitter feed shows they were active on 22nd February 2019. A pinned tweet from January states that the Aktis were working with Axiom in Somaliland, where they were visited by then UK Secretary of State for Defence Gavin Williams. There is no evidence that Axiom are in any way involved in the EXPOSE Network.

Ecorys

The EXPOSE Network distributes funds to its *'network of actors'* via its grant system. This is reportedly managed by Ecorys. They are a global research, communications services and management consultancy firm. They provide consultancy services to a range of government, supranational government and non governmental organisations. These include the EU, the World Bank, the European Investment Bank, USAID and UNICEF.

The sectors they focus upon include Security and Justice. With regard to security they state:

"Ecorys supports European security policies by providing evidence-based research, policy advice and organisational assistance on security themes and initiatives. We are partners of the European Commissions' multi-annual project on 'Community of

Users in the area of Secure, Safe and Resilient Societies'. The project promotes delivery of training projects surrounding risks such as man-made/ natural disasters, border security and terrorism."

Toro Risk Solutions

Toro Risk Solutions are named as risk managers for the EXPOSE Network. They state on their website that they offer *"Discreet, professional & competitive support to businesses, Governments & private clients."* They provide specialists services in counter terrorism, counter misinformation, intelligence, surveillance & reconnaissance, cyber defence & digital exploitation to corporate and government clients.

Toro's CEO is Peter Connolly, a listed member of the Exercise Group 7 (TEG7.) He has a British military background, having led troops on counter insurgency and counter terrorism operations in Afghanistan, Iraq, Northern Ireland, Kenya and Somalia. He developed *'Red Team Penetration Testing'* which *simulates* Wi-Fi attacks; hostile reconnaissance; surveillance; phishing; spoofing; social engineering (by phone, online and in person); physical intrusion and computer network exploitation. Presumably, these skills are a useful addition to the

EXPOSE Network's *counter disinformation* strategy.

EXPOSE Network's head of Cyber and IT is listed as Toro's Jeremy Lloyd who was also a member of the Core Project Delivery Team in the Zinc led bid. Jeremy specialises in cyber security software, having developed solutions for the financial industry. Toro state that all their staff, like Jeremy, are *"highly vetted and have a solid track record of working in corporate security and for the UK Government."*

The EXPOSE Network Head of Physical Security is a Toro consultant called Chris White. An experienced Incident/Crisis Manager for the UK government, he was a former chief of covert operations for a UK Multinational Task Force in '*non-traditional overseas environments.'*

Toro Risk Solutions are a NATO training partner. It is extremely unlikely they would do anything to jeopardise such a valuable commercial relationship.

The Institute for Statecraft

The Institute for Statecraft (IfS) appear to be in something of a hiatus. Though appearances can be deceiving. They are a registered Scottish charity. However, their previous registered charity address was a semi derelict Mill in Fife in Scotland. They are still active on Twitter but their Facebook activity tailed off in May 2019. Their Twitter use now appears to consist of no more than retweets, though it shows they remain functional in some capacity.

The IfS came to prominence in 2018 when leaked documents on the Integrity Initiative , founded by the IfS, came to light. The Integrity Initiative was directly funded by the UK government and, just like the EXPOSE Network, was a project of the Counter Disinformation and Media Development (CDMD) program, headed by Andy Pryce. Additional funding came from NATO, The Lithuanian Defence Ministry, The Smith Richardson Foundation, Facebook, the U.S State Department and others.

Claiming they were *'hacked,'* they effectively shut down their website in February 2019. The investigation into the alleged *'hacking'* was undertaken by the National Cyber Security Center, part of the Government Communications Head Quarters (GCHQ.) Unusual for a charity.

No evidence has been produced in the public domain that any *'hacking'* occurred. As is often the case, all we have are statements from government saying it happened. The Kremlin have been blamed but, without any evidence, a leak seems equally credible.

In response to the release of information the Integrity Initiative made a statement:

"The Integrity Initiative is a partnership of several independent institutions led by The Institute for Statecraft. This international public programme was set up in 2015 to counter disinformation and other forms of malign influence being conducted by states and sub-state actors seeking to interfere in democratic processes and to undermine public confidence in national political institutions……It is inevitable that a programme tackling disinformation in Europe finds itself spending much of its time addressing the activities of the Russian State, including those carried out through its intelligence services. The Kremlin has invested more operational thought, intent and resource in disinformation, in Europe and elsewhere in the democratic world, than any other single player."

Just like the EXPOSE Network it is clear the Integrity Initiative was "*tackling disinformation in Europe*." Its stated purpose was identical to that of the EXPOSE Network. Namely a *'counter disinformation'* effort, primarily directed against the Kremlin.

The Integrity Initiative's exposure led to some uncomfortable revelations for the UK Conservative Government. It appears their *'counter disinformation'* operations included interference in European democracies.

As with the EXPOSE Network the Integrity Initiative operated a *network of actors* across Europe called *'clusters.'* One such cluster in Spain, supported by others, launched a coordinated media and social media smear campaign to stop the announced appointment of soldier and academic Pedro Baños Bajo to the role of Director of the Spanish Department of Homeland Security. The Integrity Initiative were apparently willing to *"interfere in democratic processes"* themselves.

It seems they were also engaged in, among other activities, a propaganda campaign in the UK against the leader of her Majesty's Opposition, Labour leader Jeremy Corbyn. This forced a damage limitation apology, of sorts, from the one of

the directors of the IfS Christopher Donnelly. It is difficult to understand how such activity can be deemed *'counter disinformation.'*

The similarities with the EXPOSE Network continue. The Integrity Initiative network of 'clusters' employed many of the same *actors*, such as StopFake in the Ukraine, who are also recommended for inclusion in the EXPOSE Network.

Christopher Donnelly

Christopher Donnelly, co-founding director of the Integrity Initiative, is one of the implementing board members, and sits on the project board, of the EXPOSE Network. He has provided advice to four Secretaries-General's of NATO and numerous Chiefs of the Defence Staff. He's been a *'Specialist Adviser'* to three UK Defence Secretaries (both Labour and Conservative), the House of Commons Public Administration Select Committee and currently advises the Intelligence and Defence Committee. He is not the only members of the IfS who has

apparently transferred across to the EXPOSE Network Facilitator.

Ben Fellows, a Network Manager for the EXPOSE Network, was also a member the IfS team with responsibility for the Integrity Initiative's Ukraine operation, working alongside StopFake. The EXPOSE Network's Legal Advice is provided by James Wilson. He gained further experience of advising NGOs and other specialist groups across Europe on defamation, data protection, commercial contracts, corporate governance and cyber security during his time as legal advisor to the Integrity Initiative.

Just like the EXPOSE Network, it is evident the IfS were set up partly to protect the reputation of their client, The UK Government FCO. This is exemplified in another document, in the 7th Integrity Initiative leak, called Proposal To Understand and Counter Russian Active Measures:

"This project is best undertaken outside direct government control to minimise the inevitable accusation of being part of an orchestrated state-sponsored active measure. Using the IfS extensive and trusted network, including its existing Integrity Initiative, can keep the project somewhat under the radar while still accessing state and non-state actors that may not be so open with central government approaches in this area."

This *'under the radar'* approach is also common to the EXPOSE Network. Both the EXPOSE Network and the Integrity Initiative (& IfS) share the same objectives, methods, funding sources, operational management, oversight and even some of the same staff. In fact, in many regards, the EXPOSE Network appears to be the Integrity Initiative by another name. It is notable that the IfS web presence *'went dark'* only a matter of weeks before the EXPOSE Network and the OIP appeared.

EXPOSE Network Resource Partners

The Media Diversity Institute (MDI)

The Media Diversity Institute (MDI) is another UK based charity (1110263 – Media Diversity). Their beneficial purpose is stated as:

"Training for journalists; Media relations training for NGO's; training for journalism academics and setting up specialist curricula in universities; research and media monitoring."

They seem like a perfect fit for the EXPOSE Network's propaganda operations. What better way than to train journalists while they are still in university. Their media monitoring will also be useful for reporting data in real time to the UK Government, identifying '*individuals vulnerable to disinformation.'*

They say on their website that they engage with a range of *"actors in society who can influence media coverage of diversity."* These include media decision makers (owners, editors, and managers), Civil Society Organisations (CSOs), journalists and governmental organisations. They achieve this by running conferences,

workshops and courses. They publish manuals and media resources, produce online, radio, TV and print media and are active in Europe, the former Soviet States, Sub-Saharan Africa, the Middle East, North Africa, and South East Asia.

A truly amazing achievement for just four paid staff and four registered volunteers. Presumably these people are incredibly well paid. They certainly have access to the *necessary 'donor support'*.

The Council of Europe, the European Commission, the Eurasia Foundation, Dutch Ministry for Foreign Affairs, UK FCO & DfID, the Swiss Agency for Development and Cooperation (SDC), the Swedish International Cooperation Development Agency (SIDA), the Open Society Institute, the United Nations Development Program, UNESCO & the UNHCR and the Westminster Foundation for Democracy (partners of the World Bank) are among those paying four people to deliver media training across the world.

The team has become even more stretched recently. The Executive Director Melica Pesic is now on the advisory board of the EXPOSE Network, which MDI reference only as the Open Information Partnership, neglecting to mention it's the Network Hub of the EXPOSE Network. A quick look at their current projects see's that they are all very much engaged with young people in places like Jordan, Serbia and Macedonia in addition to projects, spanning entire continents,working with children's *'hearts and minds.'*

While the MDI say they advocate diversity and combat hate we can understand the kind of policies they are actually required to promote if we look at just one of their funders. The Eurasia Foundation, founded in 1992, presents itself as wonderful organisation which *"amplifies the voices of marginalized groups, particularly women, youth, minority populations, and the economically disenfranchised."* Their website is full of banal, if heart warming, corporate jargon about empowering people, building partnerships and addressing barriers.

However, we can get a more useful information if we look at a previous iteration of their website. The Eurasia Foundation makes grants for the *"accelerated development and growth of private enterprise."*

They receive the bulk of their funding from the United States Agency for International Development (USAID) and the U.S. Department of State. USAID are a funding vehicle used to promote U.S foreign policy and commercial interests. The U.S Department of State claim:

"The Department of State and USAID are indispensable tools for resolving the most difficult national security issues and protecting our (U.S. Government) freedoms"

[Note: Bracketed information added.]

At the launch of President Trump's strategy for Countering Malign Kremlin Influence (CMKI) the head of USAID Mark Green gave an address to the gathered MSM. He said:

"President Reagan [also] warned us that freedom and democracy are neither assured or inevitable. In his historic speech before the British Parliament, Reagan said, "No, democracy is not a fragile flower. Still it needs cultivating." In other words, we can never rest."

Reagan's speech came to be known as the Westminster Address. It was a pivotal moment in the history of the west's strategy for countering *Kremlin disinformation*. Something we'll discuss in more detail in Part 5. Green continued:

"At USAID, we're stepping forward to assist democracies and institutions who may be targeted by Kremlin aggression. We've crafted a framework for this assistance, that we call….CMKI…….at the heart of CMKI is our support for building the capacity of indigenous media to provide trusted, independent news and information services…..We're also supporting extensive media literacy programs in targeted countries……In Europe and Eurasia, the Kremlin's efforts are unmistakable……Thousands of Kremlin paid teams flood platforms and peddle content designed to create confusion, distrust, and cynicism about democratic and Western institutions."

President Reagan – Westminster Address

It is notable that, to date, there is absolutely no publicly available evidence at all to substantiate any of these claims about the scale of *Kremlin disinformation*. We just have to take Mr Green's word for it. In his address, Green accurately encapsulated the purpose of the EXPOSE Network. He could have been describing the work of the Media Diversity Institute too, who are also funded by USAID via the Eurasia Foundation.

In the 2020 Congressional Budget Justification for USAID spending, $628.1 million was allocated to the U.S. Agency for Global Media (USAGM). Their board include former Director of the CIA and current U.S Secretary of State Mike Pompeo. Their networks include Voice of America (VOA), RadioFreeEurope/Radio Liberty and the Middle East Broadcasting Networks (MBN).

RadioFreeEurope/RadioLiberty (RFE/RL), was created by the CIA in 1949 via its front organisation The National Committee For a Free Europe. During a difficult period for U.S intelligence, in 1972 the CIA officially withdrew their funding which then came under the purview of the the U.S. Board for International Broadcasting

(BIB). In 1994 this became the Broadcasting Board of Governors, changing it's name to USAGM in 2018. Welcoming the name change, the former CEO of the USAGM, John F. Lansing, said:

"The U.S. Agency for Global Media is a modern media organization, operating far beyond the traditional broadcast mediums of television and radio to include digital and mobile platforms. The term "broadcasting" does not accurately describe what we do……the agency's global priorities [, which] reflect U.S. national security and public diplomacy interests…..Now more than ever, people around the world need access to the truth. USAGM continues to tell the truth, and illuminate the world like no other news organization in the world."

Some of the recent '*U.S. national security and public diplomacy interests*' have been reflected in U.S. attempts at *'regime change'* in Venezuela, aimed at ousting the elected President Nicolás Maduro. As part of what now appears a faltering effort, the USAGM instigated a media campaign against the incumbent Venezuelan president. The reason for this was simply that the U.S, state wanted U.S. corporations to get their their hands of Venezuelan oil reserves. While in office, former National Security Advisor John Bolton told Fox news:

"It will make a big difference to the United States economically if we could have American oil companies invest in and produce the oil capabilities in Venezuela."

A hard nosed approach some distance away from the puritanical humanitarian aspirations of the Eurasia Foundation and the MRI.

In February 2019 it was widely reported by the MSM that deadly clashes had broken out when Maduro's forces allegedly stopped a much needed aid convoy of medicine from reaching the supposedly beleaguered people. The central

allegation, unquestioningly propagated by the USAGM media, were that the Venezuelan military had set fire to the convoy.

The western media narrative, spread with the assistance of global news agencies such as Associated Press (AP), was provably false in almost every regard. Firstly The convoy was the responsibility of USAID and they didn't list medecine but rather medical supplies, such as surgical masks, as the contents. Secondly, despite numerous fake news reports to the contrary, the Maduro government were allowing aid into the country from organisations such as the International Red Cross. Moreover, video footage and photographic evidence proved that it was the anti government protestors on the Columbian side of the border who set fire to the trucks, not the Venezuelan authorities.

It was all *'fake news.'* STRATCOM (strategic communications) or *'propaganda'* in its purest form. Thanks to independent investigative reporters and modern communication technology, enabled by the Internet, the hoax was soon exposed. "*Now more than ever, people around the world need access to the truth."*

Another example of how USAID protects U.S national security was their funding

of the ZunZuneo social media movement in Cuba. Between 2009 – 2012, via a system of shell companies and offshore banks, funds were channeled by USAID to a network of social media users with a view to fomenting dissent among young Cubans, against the Castro government. The youngsters' data was then hoovered up, almost certainly by the U.S intelligence agencies.

USAID are currently preoccupied with the Internet and digital solutions. Their sprawling partnerships and numerous initiatives aim to *"maximize the return on USAID's investment, and ensure sustainability by supporting market-driven solutions."* For example, the *Alliance for Affordable Internet* sees them partner with Google, the Omidyar Network (Luminate) and the UK Government's DfID in a *"broad coalition of governments, technology providers, civil society groups."*

Similarly their *Better Than Cash Alliance*, which seeks to do away with cash, making sure all transactions are monitored by the ubiquitous global corporate state, aligns them with the Bill and Melinda Gates Foundation, Citi, Ford Foundation, Mastercard, Omidyar Network, UNCDF and Visa. Initially they have offered their cashless transaction monitoring system to *'partners'* within the governments of Malawi, Colombia, Afghanistan, Kenya, Peru, the Philippines, and Rwanda. Maximising the return on USAID's, and American corporation's, investments.

On behalf of USAID, the Eurasia Foundation makes grants to further these U.S. national security interests. As a funder of MDI, a key resource partner in the EXPOSE network, they will be expected to ensure USAID and the U.S Department of State's commercial and political objectives are met. MDI will need to keep the EXPOSE network's *'counter disinformation'* efforts on track. Making sure they deliver on this commitment.

Objectivity, transparency, honesty and journalistic integrity are not priorities.

Neither is *counter disinformation*. What matters is that U.S. national security interests are promoted.

Digital Forensic Research Laboratory (DFRLab)

(DFRLab) is a program of the Atlantic Council. The Atlantic Council is a NATO think tank, lobby group and policy advisor. In other words, DFRLab represent NATO.

While the Atlantic Council claim they are *'independent'* they receive financial support from the U.S. Departments of State plus the Departments of the Air Force, Army, Navy and Defence. Which is another way of saying they are funded by the U.S. Government. Additional government support comes from the UK (FCO), United Arab Emirates, Denmark, Sweden, Japan, Norway and others.

The Atlantic Council are the epitome of what some call the shadow government, or deep state. This is the intertwining network of governments, NGO's, corporations and wealthy foundations which form a global web of coalescing commercial and political interests. Those who contribute to the Atlantic Council

expect to profit economically and politically from the Atlantic Council's ability to shape NATO policy.

There is no doubt about the revolving door between NATO and the *independent* Atlantic Council, nor any about its ability to influence NATO policy. For example, only six months after *'stepping down'* as NATO's Supreme Allied Commander in Europe, Gen. James L. Jones became Chairman of the Atlantic Council. He quickly formed the Atlantic Council's Strategic Advisors Group (SAG). In 2008 the group set about an ambitious NATO reform program, it's role to produce:

".....major public policy briefs and reports, host[s] off-the-record Strategy Sessions for senior U.S. and European civilian and military officials, and provide[s] informal, expert advice to senior policymakers."

The revolving door rapidly turned again for Gen. Jones and, in May 2009, he was appointed by the Obama administration as National Security Advisor on the U.S. National Security Committee (NSC).

In the meantime the SAG's report's were presented to U.S Senate Foreign Relations Committee among others; they briefed military and civilian leaders at NATO headquarters; between 2008 to 2010 they attended all five official NATO conferences on the New Strategic Concept and were co hosts of the Washington Conference at the National Defense University with then NATO Secretary General Anders Fogh Rasmussen, Defense Secretary Robert Gates and the Secretary of State Hilary Clinton, in attendance.

In a fairly typical example of how the Atlantic Council operate, Gen. Jones had essentially been seconded to them to set up the SAG. The SAG produced the reports that influenced policy makers to support NATO's New Strategic Concept.

With the political will secured, Jones was then appointed to government to make sure the NATO policy, he had played a major role in creating, was implemented.

Gen. James L. Jones

The Atlantic Council offer a corporate program allowing private corporation to partner with NATO. Their Convene, Connect, Colaborate (CCC) program:

"….engages the private sector as a crucial partner. Through substantive partnerships, networking opportunities, event sponsorship, and corporate membership, the program provides partners unique opportunities to achieve business and corporate responsibility goals."

These partners, via CCC and other Atlantic Council *'programs,'* include the defence contractors Raytheon, Lockheed Martin, Boeing, Thales Group, Northrop Grumman and MBDA. So what *business goals* might they hope to bolster through their partnership with NATO?

To date, the War on Terror is conservatively estimated to have cost in the region of $6 Trillion in the U.S. alone. This tax revenue then flows into the coffers of the defence contractor's major shareholders. From a financial perspective, it's as simple as that.

The War on Terror started, not in response to the attacks on the September 11th 2001, but rather as a result of the attribution of guilt for those attacks. The whole basis for a global war against Islamist extremists, costing millions of lives, was predicated upon this determination of culpability.

On September 12th the NATO Council of member states met to express their willingness to stand behind the U.S. This included a possible invocation of Article 5 of the Washington (NATO) Treaty. This broadly stipulates that an attack against one member state can be deemed an attack against all. It authorises a range of possible responses, including military action.

Lord Robertson Sec. Gen. NATO 2001

The War on Terror began in earnest when then NATO Secretary General Lord Robertson gave a public address on October 2nd 2001. Under Article 5, from that

point on, the NATO coalition were embroiled in conflict against, what was then, a largely invisible enemy. Lord Robertson stated:

"This morning, the United States briefed the North Atlantic Council on the results of the investigation into who was responsible for the horrific terrorist attacks which took place on 11 September. The briefing was given by Ambassador Frank Taylor, the United States Department of State Coordinator for Counter-terrorism.

Today's (briefing) was [a] classified briefing and so I cannot give you all the details. Briefings are also being given directly by the United States to the Allies in their capitals.

The briefing addressed the events of 11 September themselves, the results of the investigation so far, what is known about Osama bin Laden and the Al-Qaida organisation and their involvement in the attacks and in previous terrorist activity, and the links between Al-Qaida and the Taleban regime in Afghanistan.

The facts are clear and compelling. The information presented points conclusively to an Al-Qaida role in the 11 September attacks.

We know that the individuals who carried out these attacks were part of the world-wide terrorist network of Al-Qaida, headed by Osama bin Laden and his key lieutenants and protected by the Taleban."

[Note: Bracketed informationa added]

So the message was clear and unequivocal. Following a thorough investigation by the U.S Department of State, Ambassador Frank Taylor gave oral briefings to

NATO, reporting the hard evidence proving al Qaeda's guilt and their links to the Taliban. All the evidence is secret but NATO found the facts *'clear and compelling.'* This provided the legal basis for the U.S. led invasion of Afghanistan and then the wider War on Terror, still raging today.

Ambassador Frank Taylor

Frank Taylor's oral briefing notes were declassified in 2009. Called *"Working Together To Fight The Plague of Global Terrorism"* and dated October 1st 2001, the day before Robertson's address. It is undoubtedly the briefing referenced. We know this because the *"the Allies in their capitals"* are the listed recipients and a section of the report was copied and pasted directly into the NATO Secretary General's speech:

"The facts are clear and compelling…….We know that the individuals who carried out these attacks were part of the world-wide terrorist network of Al-Qaida, headed by Osama bin Laden and his key lieutenants and protected by the

Taliban."

So what was the evidence NATO found so compelling?

Nothing! There is no evidence at all anywhere in the document that links either al-Qaeda or Ossama bin Laden to the 11th September attacks. There are an awful lot of statements, assertions and claims but no actual evidence. In no way does it come anywhere near to the standard of evidence required in a magistrate's court, let alone the NATO Council.

For example, one of the alleged terrorists was supposedly identified from the flight manifests as Kalid al Midhar. The U.S. State Department then point out that they have intelligence that someone identified as *"Khalid the Saudi"* may have had something to do with the East Africa Embassy bombings. Therefore this must be the same Khalid al Midhar because he too was a Saudi called Khaled. Apparently the U.S. State department have information which identifies him as an al-Qaeda operative. They just don't say what it is.

If you read the document hoping to find something more substantial, you will be disappointed. Yet NATO were sufficiently convinced to authorise a global conflict, on numerous fronts, off its back.

No wonder multinational corporations, governments and their NGO's are queuing up to give some *'donor support'* to the Atlantic Council. It appears NATO will believe anything. If your aim is to profit from war, you are on to a winner.

NATO class disinformation as being part of something they call hybrid warfare. This is the blurring of the lines between war and peace General Carter spoke of recently. When war is peace, perpetual war is guaranteed, as are related profits.

To this end, *"NATO is strengthening its coordination with partners, including the European Union, in efforts to counter hybrid threats. It also actively counters propaganda – not with more propaganda, but with facts – online, on air and in print."*

Throughout their technical proposal Zinc were very keen to highlight the exemplary work of DFRLab and to stress they were on board with the EXPOSE Network project. They say they are *vital* and *'global leaders in tracking disinformnation,'* that they *set standards* and are *experts.* However, given the measure of evidence acceptable to the Atlantic Council and NATO we might have some reservations.

This summer, NATO's self proclaimed *Digital Sherlocks* released their report into an alleged *Kremlin disinformation* cell they called Operation Secondary Infektion. There is no such operation by the way, it's just a name DFRLab made up. Most people might expect a *'forensic investigation'* to analyse the available evidence, giving clear citation and attribution and then form a meaningful conclusion based upon the known evidence. That is not what DFRLab did.

DFRLab made some dramatic claims:

"The Atlantic Council's Digital Forensic Research Lab (DFRLab) uncovered a large-scale influence operation that spanned nine languages, over 30 social networks and blogging platforms, and scores of fake user profiles and identities…..The scale of the operation, its tradecraft, and its obsession with secrecy, indicate that it was run by a persistent, sophisticated, and well-resourced organization……"

They add:

"Possibly an intelligence agency."

Possibly I suppose but, using Occam's Razor, probably not.

DFRLab claim their investigation was based upon Facebook's discovery of a *"small network of fake accounts emanating from Russia."* They can't be certain they were Russian because *"DFRLab does not receive access to Facebook's backend data."*

DFRLab decided they probably were Russian because *"contextual and linguistic points helped to corroborate Facebook's attribution to a likely Russian source."* These accounts were said to be spreading disinformation. However, *"there were only 16 accounts, and their posts had little impact."*

So Facebook appear to have identified a small, ineffectual group of accounts posting stupid stuff on their platform. They may or may not have been Russian. Their English wasn't great so they were probably not from an English speaking country. Their syntax indicated they might be Eastern European, or possibly even Russian. No one knows for sure.

According to DFRLab this was just the *'tip of a much larger iceberg.'* They claim the iceberg was *"operated from Russia."* Unfortunately, they don't present a scrap of evidence to substantiate any of this.

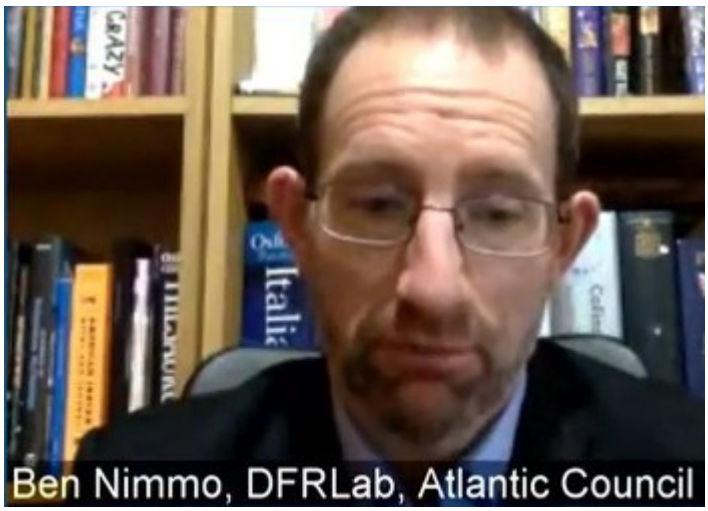
They allege *"The operation was ambitious, although its reach was small."* So not so much of an iceberg, more of an ice cube. It also begs the question, if its reach was small, how DFRLab knew the scale of its ambition? They go on:

"Fortunately, almost none of the operation's stories gained traction. Some were ignored; others were mocked by forum users as soon as they were posted, in a welcome sign of public awareness of the dangers of disinformation."

In that statement DFRLab managed, not only to utterly undermine their own ludicrous claims, but also the entire *Kremlin disinformation* narrative and the whole reason for the supposed existence of the EXPOSE Network. Despite having no reason to do so, let's accept DFRLab's story for a moment. If a network of Russian disinformation operatives are posting information online, which doesn't gain any traction and ends up either being completely ignored or mocked, what on Earth do the public need to pay the EXPOSE Network for?

As if that wasn't enough, DFRLab add:

"Open sources cannot attribute this operation to a particular Russian actor with high confidence, although the approach and tradecraft resemble an operation by an intelligence service."



Ben Nimmo (Kremlin Disinformation expert?)

If OSINT can't tell the difference between an SVR agent, spinning online propaganda, and a stoned Lithuanian teenager, winding people up on Reddit for a laugh, what use is it? This abject bilge continues for more than 60 pages. Listing numerous spoof accounts and fake stories which literally anyone could have posted. Tenuous links are drawn between alleged 'networks' (no evidence provided) as the whole random heap of jumbled rubbish ends in its depressingly irrelevant conclusion:

"More research would be needed to verify the attribution."

Two of the co-authors of this publication, which they have the audacity to call a report, are Benn Nimmo and Graham Bookie. Both Benn and Graham are on the interim advisory panel of the EXPOSE Network. Perhaps more worryingly Eric Toler, from DFRLab, is the EXPOSE Network's Open Source Researcher and Trainer.

Sold by Zinc as the vital experts at the forefront of the imagined battle against

conspicuously absent *Kremlin disinformation,* if their Operation Secondary Infection *'report'* is anything to go by, DFRLab's ability to investigative evidence and form a rational conclusion, is minimal. You have to wonder if the EXPOSE Network even believe *Kremlin disinformation* to be a threat.

They don't seem that interested in investigating what little evidence there is for genuine Russian propaganda operations. Perhaps doing so would simply reveal their relative impotency. The EXPOSE Network's agenda appears to be to guide the public towards whatever objective NATO, USAID, the U.S. State Department and the vast array of government and corporate interests behind them, wish to achieve.

Something which becomes even more evident when we look at the two remaining resource partners, Bellingcat and Zinc Network. Which we do in the next Chapter.

Chapter 6: The EXPOSE Network Partners (Continued)

Thus far we have looked at the EXPOSE Network and its Hub, the Open Information Partnership (OIP); we've considered the role of the EXPOSE network, authenticated the supporting evidence and examined how a consortium, led by Zinc Network, will operate as the Network Facilitator.

In Part 4 we started the process of unpicking the web of interconnected NGO's, intelligence agencies and multinational corporations behind EXPOSE. This demonstrated that available resources far exceed those suggested by the disclosed £10 million, three year contract. In addition, the potential pot of EU funding directed towards countering *Kremlin disinformation* is vast in comparison to the stated EXPOSE Network's budget. Something we consider in the next, concluding part of the series.

In his 1982 Westminster Address U.S. President Reagan said:

Smitten with deregulation

"We have not inherited an easy world……the gifts of science and technology have made life much easier for us, they have also made it more dangerous…… While we must be cautious about forcing the pace of change, we must not hesitate to declare our ultimate objectives and to take concrete actions to move toward them….

…The objective I propose is quite simple to state: to foster the infrastructure of democracy……We in America now intend to take additional steps…… [the]..Republican and Democratic party organizations are initiating a study with the bipartisan American Political Foundation to determine how the United States can best contribute……to the global campaign for democracy now gathering force….

….It is time that we committed ourselves as a nation – in both the public and private sectors – to assisting democratic development……..There is a proposal before the Council of Europe to invite parliamentarians from democratic countries to…..consider ways to help democratic political movements….

…The task I have set forth will long outlive our own generation……Let us now begin a major effort to secure the best – a crusade for freedom that will engage the faith and fortitude of the next generation."

Reagan was declaring a new form of conflict, one fought with the weapons of information, disinformation and propaganda. No distinction would be drawn between peace and war. The war would be perpetual. The objective was to undermine the political and economic institutions of the enemy from within; to seed ideology among populations and foster movements for *democratic development*; to confront all who oppose the neoliberalism of the western corporate state.

Combining the might of both the state and private corporations, the force fighting this hybrid warfare would be both overt and covert. Today we call this public private partnership *"soft power."*

Private partnership is essential if the project is to work. In the UK just three corporations (News UK, Daily Mail Group & Reach) control 83% of the news media. With the addition of The Guardian and the Telegraph, nearly 80% of the online news coverage is also under corporate control. Similarly, in the U.S. six corporations control 80% of the people's free and open mainstream media (MSM).

From everything we've learned about the EXPOSE network it is clear that combating *Kremlin disinformation,* if an objective at all, is not its primary focus. It is part of a wider strategy, envisaged in Reagan's Westminster Address, for controlling the flow of information in order to overwhelm resistance to the global corporate hegemony. The corporate state or *'corpratocracy.'*

Now we'll consider how the remaining two resource partners of the EXPOSE

Network have been tasked to deliver on this commitment.

Bellincat

Bellingcat is probably the best known of the EXPOSE Network partners. It's founder Eliot Ward Higgins has been featured on numerous mainstream media (MSM) programs. Almost as soon as he started writing his blog, the MSM began to promote him. This makes him practically unique in the political blogosphere. Few, if any, receive this kind of media attention so quickly. There are some well known political bloggers who have gradually built significant followings, achieving a modicum of impact, but none have gone on to write NATO approved reports, other than Higgins.

Bellingcat is an allegedly independent journalism platform started by the blogger Higgins. He began writing, while unemployed in 2012, under the pen name 'Brown Moses.' After receiving considerable MSM exposure, in July 2014 Higgins launched a KickStarter fundraiser for Bellingcat as a platform for *'citizen journalists.'* In just 32 days he raised an impressive £50,891 from 1701 backers to get his new blog off the ground. The backers remain anonymous. Bellingcat was incorporated in November 2015, limiting its director's liabilities.

Eliot Ward Higgins

Higgins' carefully crafted Wikipedia legend claims he pioneered the process of monitoring multiple social media channels to gather information from sources such as YouTube. However, the use of online tools to do this was common practice across the blogosphere in 2012. Bellingcat is frequently cited as a leading exponent of open source intelligence (OSINT.) DFRLab's Operatioan Secondary Infektion being an example of what OSINT can achieve.

In October 2015, just over a year after launching Bellingcat (a blog), Higgins was a lead contributor to the Atlantic Council's report Hiding In Plain Sight. With his star rising at meteoric pace, by 2016 Higgins was made senior fellow at the Atlantic Council. He was soon a lead contributor on the Atlantic Councils' 2017 publication Breaking Aleppo. Notably, Higgins left this role as his partnership with the OIP began.

Listed contributors to Breaking Aleppo report included the White Helmets and the

Aleppo Media Centre, now defunct. The White Helmets were founded by ex British Military Intelligence Officer (MI5) James Le Mesurier and are strongly linked with numerous terrorist organisations including al Qaeda and ISIS. They are directly funded by the U.S and UK government Foreign and Commonwealth Office, who also fund the OIP hub of the EXPOSE Network.

The Aleppo Media Centre were backed by the French state broadcaster Canal France International. The AMC acted as a terrorist media hub during the occupation of Aleppo. The kind of propaganda they created included the false attribution of images, the editing of video to remove incriminating evidence, the falsifying of casualty reports and so on.

Omran Daqneesh

One of the AMC's most iconic images was the picture of the child Omran Daqneesh which the AMC syndicated globally. The Photo was taken by AMC linked photo journalist *'freelancer'* Mahmoud Razlam. Raslan was a supporter of

the *'terrorist'* group Nour al-Din al-Zenki who filmed themselves beheading a young boy called Abdullah Issa.

Nour al-Din al-Zenki are claimed by the western coalition of NATO states to be a moderate rebel group. Yet they joined with the al-Qaeda umbrella group Hay'at Tahrir al-Sham (HTS), formerly Jabhat al Nusra (al-Qaeda in Syria) before merging with Ahrar al-Sham to form the Syrian Liberation Front. Ahrar al-Sham were former allies of ISIS until a spat in 2014 saw them form an allegiance with Jabhat al Nusra in opposition to Islamic State. Obviously, calling Nour al-Din al-Zenki *moderate rebels* is preposterous.

Nour al-Din al-Zenki's public beheading of a child prompted some questions but the British state broadcaster, the BBC, leapt to their defence. They wrote an anonymous propaganda piece justifying the barbarity. They claimed the small boy was *'a fighter'* and suggested he was *'considerably older'* than he looked. Abdullah Issa was 12 when he was decapitated by the U.S. led coalition's *'moderate rebel'* allies.

So it is not without reason we might question why Mr Higgins would associate Bellingcat with such people. Similarly we should also question the impartiality and *'fact checking'* of an Atlantic Council report written with their assistance. Bellingcat will be central to the EXPOSE Network's effort to provide *"trustworthy facts and sources for everyone."*

Bellingcat state on their about page that their partners include the supposed NGO the National Endowment for Democracy (NED). An organisation with extensive links to the U.S. Government, globalist think-tank's, multinational corporations and western intelligence agencies.

Higgins stated that his interest in geopolitics was prompted by the news coverage of the Arab Spring. This was generally reported as an organic uprising of grassroots activist movements demanding greater democracy and political change in the Middle East and North Africa.

Starting in Tunisia, within little more than a few months, similar uprisings occurred in Bahrain, Egypt, Libya, Syria and Yemen. All of them led to widespread violence and political upheaval with horrific military conflicts soon breaking out in Libya, Syria and Yemen.

National Endowment for Democracy

The Arab spring started in 2011 but in in 2008 activist leaders, such as those from Egypt's April 6 movement, were in New York for the first Alliance of Youth Movements (AYM) conference. The AYM was sponsored by, among others, Google and Facebook (both NED donor supporters) and the U.S. Department of State. Numerous corporate executives and government official attended to give their support to the enthusiastic youngsters.

Shortly thereafter, in 2009, the activists were sent to Serbia where they received additional training from the Centre for Applied Nonviolent Action and Strategies (CANVAS). CANVAS are supported by a number of organisations dedicated to political change. Among them are IREX, who also donate to the EXPOSE Network's partner the Media Diversity Institute.

IREX are supported by Google, Facebook, the Open Society Foundation (who also support Bellingcat) and many, many other global corporations and NGO's. IREX also enjoy the *'donor support'* of the USAID, the U.S. Department of State, the UK Foreign and Commonwealth Office (the EXPOSE Networks *'client'*) and the World Bank. All of whom were eager to support April 6's struggle for freedom.

While these revolutionary movements attracted many innocent people, who genuinely wanted reform, their organisational structures and leaderships were not remotely *'grassroot.'* These attempted revolutions were orchestrated from overseas and the National Endowment for Democracy were at the heart of most of it. This was widely acknowledged, even the MSM were forced to tentatively admit U.S. backing of the uprisings.

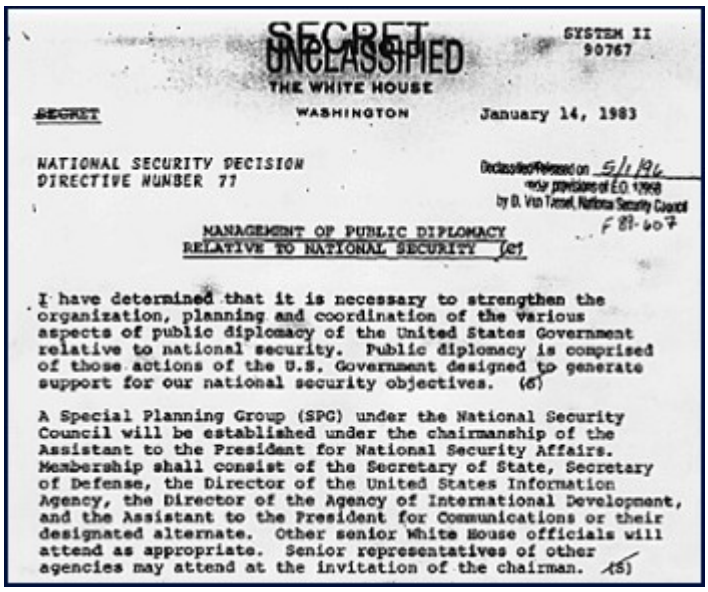
Numerous civil society organisations, all funded by the NED, such as the International Republican Institute, the National Democratic Institute and Freedom House were involved in the longstanding U.S plan. The objective, from a U.S. foreign policy perspective, was to train, equip and network significant

numbers of North African and Middle Eastern activists as part of a geopolitical strategy to undermine regional government, foment dissent, destabalise and then seize control of the targeted nations.

The primary objective of the U.S. orchestrated Arab Spring appears to have been to allow global corporations to run the targeted nation once they were reduced to chaotic, failed states. For example, following the UK / French led NATO destruction of Libya, an international oil conglomerate put their man Abdurrahim el-Keib in charge.

Just because an NGO provides support for a media outlets, *counter disinformation* project or blog, it doesn't mean the recipient necessarily share the goals or methods of the NGO. However, it is naive to imagine the funding is unconditional. In any event, it appears Higgins was a perfect fit for the NED from the start.

The NED receives an annual appropriation from the U.S Department of State and was formed during the Reagan administration as a supposedly Non-Governmental Organisation (NGO). However, it is really a government organisation whose purpose is to project U.S foreign power.



SECRET
UNCLASSIFIED
SYSTEM II
90767
THE WHITE HOUSE

~~SECRET~~ WASHINGTON January 14, 1983

NATIONAL SECURITY DECISION
DIRECTIVE NUMBER 77

Declassified/Released on 5/1/96
under provisions of E.O. 12958
by D. Van Tassel, National Security Council
F 89-607

MANAGEMENT OF PUBLIC DIPLOMACY
RELATIVE TO NATIONAL SECURITY (U)

I have determined that it is necessary to strengthen the organization, planning and coordination of the various aspects of public diplomacy of the United States Government relative to national security. Public diplomacy is comprised of those actions of the U.S. Government designed to generate support for our national security objectives. (U)

A Special Planning Group (SPG) under the National Security Council will be established under the chairmanship of the Assistant to the President for National Security Affairs. Membership shall consist of the Secretary of State, Secretary of Defense, the Director of the United States Information Agency, the Director of the Agency of International Development, and the Assistant to the President for Communications or their designated alternate. Other senior White House officials will attend as appropriate. Senior representatives of other agencies may attend at the invitation of the chairman. (U)

Presidential Directive 77

The NED was created as a result of Presidential Directive 77 which tasked the Special Planning Group, within the U.S National Security Council, to deliver *"public diplomacy activities,"* which is diplomatic code for propaganda. The National Endowment for Democracy was the result.

Comprising of four committees, the NED came into being under the auspices of the International Information Committee and the International Political Committee. The stated objective of the Information Committee were:

"…planning, coordinating and implementing international information activities in support of U.S policies and interests relative to national security. It will assume the responsibilities of the existing "Project Truth" Policy Group."

The political committee was tasked with the following:

"…planning, coordinating and implementing international political activities in support of U.S policies and interests relative to national security. Included among such activities are aid, training and organisational support for foreign governments and private groups to encourage the growth of democratic political institutions and practices."

The U.S political class deemed the creation of NED (and other NGO's) necessary due to a series of scandals that rocked the U.S intelligence community throughout the 1970's. Watergate, the Church committee into Operation Mockingbird, the Pike committee and the Rockefeller Commission all led to a political cold feet. It was expedient to put some distance between political oversight of the intelligence agencies and their activities. Plausible deniability was required.

The NED was created specifically to meet this need. To fund various operations, via its system of *'grants'* which the politicians and intelligence agencies, primarily the CIA, would prefer to disavow. Declaring itself a Non Governmental Organisation (NGO), while receiving direct state funding, was merely an exercise in public relations.

The cofounder of the NED was Allen Weinstein, he was member of the board of directors of the American Political Foundation (Democracy Program), referenced by Reagan in Westminster, which publicly established the NED. Weinstein was the inaugural NED acting chairman. Speaking to the New York Times in 1991 he said:

"A lot of what we do today was done covertly 25 years ago by the CIA"

Allen Weinstein

There is little doubt that the CIA partner the NED. Former CIA director William Casey wrote a memo to White House Presidential advisor Edwin Meese advocating the creation of the NED. He stated:

"We here (the CIA) should not get out front in the development of such an organization, nor do we wish to appear to be a sponsor or advocate."

[Note: Bracketed information added]

This echoes the sentiments outlined in Presidential Directive 77 that the NED should be a conduit for the covert funding of foreign political movements and propaganda assets, laundering the money through its NGO status. Via its grant system, the NED shapes and influences public opinion, policy and global events. An approach shared by the EXPOSE Network, with NED representative

Bellingcat's assistance.

While NED promotes U.S national security interests, these frequently coalesces with U.S corporate interests. In order to appreciate this we need only look at the network of corporations who also provide support for the NED.

A document released in 2013 showed that NED received *'generous support'* from Microsoft, Google, Chevron, Goldman Sachs and the U.S Chamber of Commerce. The 2014 Report listed other notable donors including the George Soros' Open Society Foundation and the Smith Richardson Foundation (SMF). The SMF is also a listed donor to the UK propaganda operation the Integrity Initiative along with Facebook, another NED supporter.

The NED doesn't make grants to anyone who doesn't support "*U.S policies and interests relative to national security."* Bellingcat, a resource partner of the EXPOSE Network, wouldn't receive a dime from the NED if it didn't promote the same interests. As a significant partner in the OIP, who declare "*every one of us has the right to be properly informed*," you should be aware of this. Any claim by Bellingcat that they are impartial, objective or transparent should be judged accordingly.

Zinc Network

Zinc Network were incorporate on 16th March 2018, with their domain name established the previous day. The nature of their business is public relations & communications activities and management consultancy (other than financial management). Their named officers are Scott Wayne Brown & Robert Stephen Elliot and their listed address was changed on 20th June 2019 to an anonymous office building in London.

The Open Information Partnership domain name was registered by Breakthrough Media on 28th February 2019. Breakthrough Media Network were incorporated on 21st July 2008. Their named officers are Scott Wayne Brown & Robert Stephen Elliot and their listed address is the same anonymous office building in London.

Interestingly, the CIA currently host most of their online national security infrastructure with Amazon cloud web services (AWS) *'secret region.'* By 2021 they hope to diversify this multi-billion dollar hosting contract. The OIP, Breakthrough Media and Zinc Network websites are all hosted on AWS. This

could be just a coincidence.

Zinc Network is apparently part of the Breakthrough Media and Communications Network (BMCN). Suggesting it is a subsidiary of Breakthrough Media. Yet when you go to breakthroughmedia.org, their publicly listed website, it no longer exists. Internet archives show that Breakthrough Media's website was redirecting to Zinc Network by 22nd May 2019 with a message saying *"Breakthrough Media is now Zinc Network."*

It appears that claims that Zinc is part of BMCN are somewhat disingenuous. Zinc Network is the new name for Breakthrough Media. In order to understand who Zinc Network are we need to look at the activities of the Breakthrough Media Network. They are the same company in all but name.

Robert Elliot – *'Change Agent'*

Robert Elliot , co-founder and CEO of Zinc Network, has a media background as a former TV director and producer. As CEO of BMCN *"he still retains a hands-on role in helping shape the campaigns and communications projects around the needs of the clients and the communities Breakthrough and ZINC Network supports."*

Robert, who apparently likes to call himself a *'Change Agent,'* will presumably have a *'hands-on role'* shaping the activities of the EXPOSE Network around the needs of the client, the UK Government Foreign and Commonwealth Office (FCO) and their Counter Disinformation and Media Development Program (CDMD). Robert has written articles for the Guardian among other MSM outlets.

Scott Brown is the other co-founder and Executive Director of Zinc Network. Scott says he founded Zinc Network in 2012, although it wasn't registered as a company for a further six years. He says he has lived and worked in Iraq, Somalia, the UAE and Kenya. His LinkedIn profile lists his work history:

- 2007-2008 Accounts Director at M&C Saatchi
- 2008 – 2009 Head of Internal Communications at Majid Al Futtaim.
- 2009 – 2012 Deputy Chief of Staff at Chimes Communications Ltd.
- 2012 – Date Chief Executive Officer (CEO) of Breakthrough media

So it appears Scott founded Zinc Network in 2012 while he was the CEO of Breakthrough Media. However, there are a couple of notable omission from Scott's work history. He worked for the UK Conservative Party's strategic

communications team. Presumably it was during this time that Scott first crossed paths with Richard Chalk who also worked for them.

However, Scott says he didn't encounter Chalk until they met in 2006, when both were part of PR firm Bell Pottinger's partnership with the U.S. Information Operations Task Force (IOTF) in Baghdad. This probably accounts for his time living and working in Iraq.

Scott Brown – former Deputy Chief of Staff for Bell Pottinger

Scott said he only bumped into Chalk because Chalk had been part of the management team while he had been in a lowly administrative role. So it was quite a career leap for Brown when he went from an administrative role to Accounts Director at M&C Saatchi the following year. Though possibly not, given that Scott's minor role at Bell Pottinger was Deputy Chief of Staff.

Bell Pottinger were paid by the Pentagon to produce propaganda in Iraq. The

contract, reportedly worth more than half a billion dollars, included creating fake terrorist videos with an embedded codec to identify the IP address of the viewer. They were distributed by U.S troops, to track whose hands they fell into, according to former Bell Pottinger whistle-blower Martin Wells. Wells was headhunted and joined the Bell Pottinger team at the U.S. Military base Camp Victory, in the summer of 2006.

Lord Tim Bell, also a former spin doctor for the Conservative Party, and chairman of Bell Pottinger during the propaganda operation, told reporters, *"it was a covert military operation.....It was covered by various secrecy documents.....We were very proud of it."* He confirmed that Bell Pottinger reported to the Pentagon, the CIA and the U.S. National Security Council on its work in Iraq. For their part, the Pentagon confirmed Bell Pottinger were contracted to them on the project.

For some reason, Scott Brown neglected to mention his time with Bell Pottinger on his LinkedIn profile. Nor do Zinc Network make any mention of their history on their website, remarkably claiming instead to have *"unprecedented access to the world's information."* Perhaps we shouldn't expect the *"open information exchange"* promised on the OIP website.

In 2008 Scott left M&C Saatchi and joined the Majid Al Futtaim group. They are an UAE holding company based in Dubai. Accounting for his time in there.

By coincidence, Richard Chalk became the Chief Executive of M&C Saatchi's Middle East operation the same year. He worked to establish their first Middle East office in Abu Dhabi. The project reached fruition in 2012 with a client list including the Majid Al Futtaim group.

Richard Chalk, Scott's former colleague in at least two of his roles, who he barely

knows, is the current head of the the Home Office's Research, Information and Communications Unit (RICU). Chalk became the head of RICU in 2012, the same year that Scott Brown became the Director of Breakthrough Media and, according to him, set up Zinc Network. Following Chalk's appointment, RICU began outsourcing much of their operation to Breakthrough Media.

RICU is based in the UK Home Office's Office for Security and Counter-Terrorism (OSCT), a unit set up by former MI6 officer Charles Farr in 2007. In 2011 the UK Government reviewed their Prevent Strategy. This resulted in a duty, under Section 26 of the Counter-Terrorism and Security Act 2015, for all local authorities to have *"due regard to the need to prevent people from being drawn into terrorism"*. Under schedule 6 of the act that duty extends to all providers of criminal justice, School, Local government, NHS and police services.

The Prevent Duty Guidance for local authorities outlines the UK Government's claims that potential terrorists are first drawn into *"extremist ideology."* The Prevent Strategy was redesigned in 2011 because *"non-violent extremism"* apparently creates the conditions for terrorism. So what is '*extremism'* according to the UK State?

"Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs."

They clarify:

"The strategy also means intervening to stop people moving from extremist (albeit legal) groups into terrorist-related activity."

This shifting of the goalposts from *'terrorism,'* which is both illegal and something we should take steps to prevent, to *'non-violent legal opposition to fundamental British values'* is vital to understand. Mainly because the UK state don't make any distinction between the two.

List of British values?

We know the state determines British values to *include* certain elements. These are religious & cultural tolerance, mutual respect, individual liberty, democracy and the rule of law. All commendable but lacking definition. Does this mean questioning the electoral or justice systems marks you out as a terrorist? However, *'include'* implies there are other values we don't know about. So what are they and who decides what they are? We just don't know.

There are some values that are conspicuously absent. Freedom of expression, the right to a fair trial by a jury of your peers, innocence until guilt is proven and freedom of the press aren't mentioned at all. Aren't these *British values*?

Freedom of speech is mentioned, BUT……*"it is important to realise that the risk of radicalisation in institutions does not just come from external speakers. Radicalised students can also act as a focal point for further radicalisation through personal contact with fellow students and through their social media activity. Where radicalisation happens……..these signs can be recognised and responded to appropriately."*

Much like the EXPOSE Network's *counter disinformation* program, the applied definitions, far from tackling genuine threats, all point towards a concerted effort to stop any criticism of the state and, by extension, its private corporate partners. It is the almost total lack of acknowledgments of our freedoms that stands out. It is oppressive.

Breakthrough media (Zinc Network) were tasked with creating reams of material to both promote the Prevent strategy and make sure local authorities were on board. This included promotional films, Twitter feeds, Facebook profiles, YouTube

clips, online radio content and websites. It was lucrative for Breakthrough, earning them £11.8 million in 4 years.

Breakthrough's approach to the Prevent strategy was remarkably similar to the one they have adopted for the EXPOSE Network. They reportedly aimed to *"influence online conversations by being embedded within target communities via a network of moderate organisations that are supportive of it's goals."* We can already guess who those supportive organisations might be.

David Anderson QC

In 2016 David Anderson QC was asked to conduct an independent review of terrorism laws by the Home Affairs Select Committee Inquiry into Government's Counter-Terrorism Strategy. As an employee of the state (all QC's are) his report was surprisingly frank. He highlighted many of the concerns expressed by people

(mainly Muslim community members at the time) subjected to the Prevent Strategy.

This included comments from a large scale 2015 academic review who noted that Prevent, *"reinforces an 'us' and'them' view of the world, divides communities, and sows mistrust of Muslims."* They recommended the Government should *"end its ineffective Prevent policy and rather adopt an approach that is based on dialogue and openness".* Other notable criticisms included that it *"unfairly targets Muslims and school children,"* and is used to *"spy and denigrate the Muslim community and cause mistrust".*

There is little doubt Breakthrough were creating disinformation, propaganda and operating online under a variety of spoof profiles, disseminating disingenuous and misleading content. They seemingly attracted employees under false pretenses, manipulating some into signing the Official Secrets Act, ensuring their silence, and set them to work on projects they became increasingly uncomfortable with.

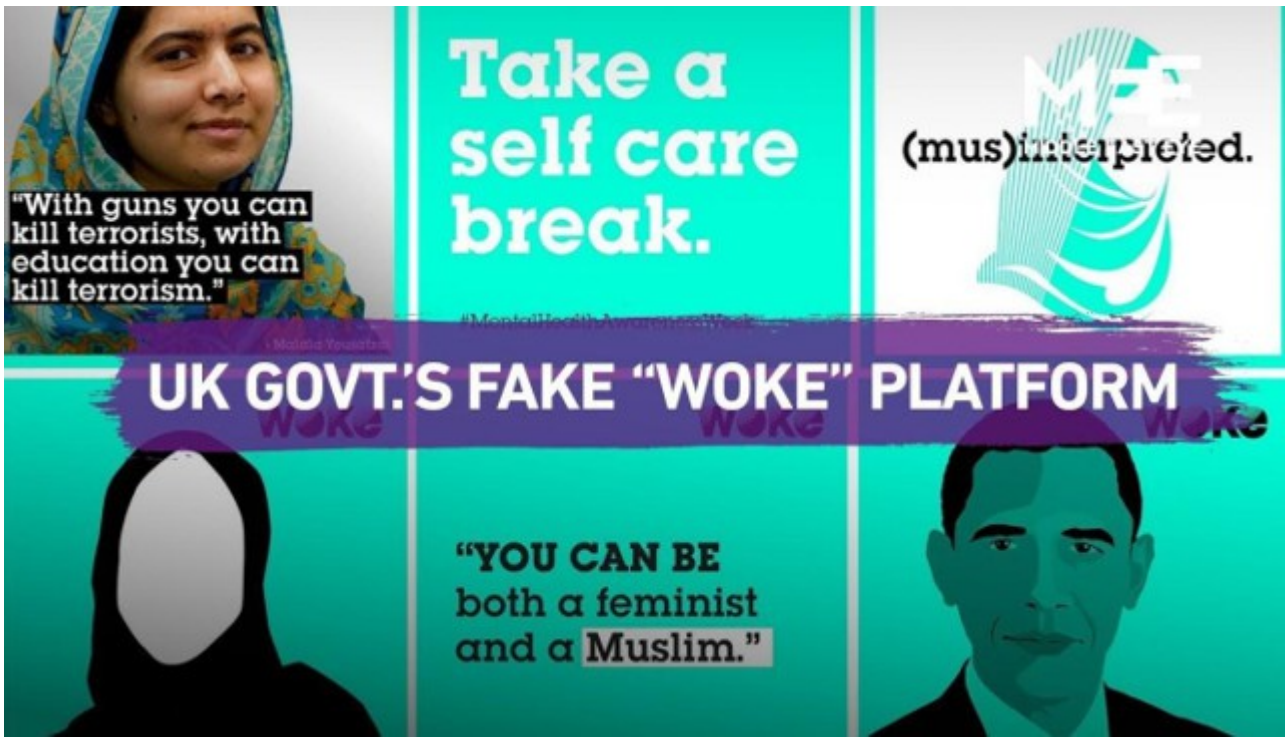
Amina Aweis was an A'level student attracted to a digital marketing and business apprenticeship scheme. She joined hoping to get some valuable training and experience and was pleased to be matched with a role as a social media manager for Zinc Network. Unfortunately the experience she gained wasn't what she anticipated.

She reports that the interview was misleading, making no mention of Breakthrough media or their government contract, instead selling her the Zinc concept as a *"grassroots organisations."* She signed the Official Secrets Act without fully appreciating, or being told, its implications. Marketed to her as an independent project her suspicions were first aroused when Breakthrough Media was referenced in office discussions.

These deepened when she realised that colleagues were creating content with fake personas, often acting as Muslim women, which predominantly they weren't. Client (RICU) meetings were held discussing engagement with the Muslim community, using her ideas, while Amina, who is a Muslim woman, was excluded. She noted political agendas, overqualified people pushed aside and freelancers being exploited. She left disillusioned and exhausted.

I have absolutely no idea if Amina's story is true. Presumably, as she signed the OFA, that's not her name. But it *"fits the narrative".* Which, apparently, is perfectly acceptable.

Eventually Breakthrough Media's (Zinc's) disinformation and propaganda program was exposed with the revelations over the WOKE program. These certainly lend plausibility to Amina's account. Presented as a distinct media company, it misled users and participants into believing its objective was to *"engage in critical discussions around Muslim identity, tradition and reform."*



In reality it was a psyop operation run by the OSCT (almost certainly RICU) with its social media operation managed by Zinc Network. Among its many utterly duplicitous creations, was a Zinc run Facebook page called "What is fake news?" It featured young Muslims saying thing like *"online, we can never know who the source is"* and *"we have to train ourselves against what's going on out there".*

When journalists used the Freedom of Information Act to request further detail from the OSCT their requests were denied, citing reasons of *'national security.'* The OSCT stated they did hold information but couldn't release it because it would:

"…open up detailed information about organisations and individuals who are engaged in the delivery of, and who are supporting activities to prevent terrorism"

We must ask ourselves how running mass media disinformation campaigns against the public protects *'national security.'* There would appear to be no

justification for this whatsoever. Sadly, if that were not bad enough, it raises another far more sinister possibility.

Charles Farr Mi6 Officer who created the OSCT

Anyone who is familiar with the evidence of Al Muhajiroun's activities in the UK must be aware of the UK intelligence agencies apparent toleration, if not support, for their Islamist extremist recruitment operations. If you wish to radicalise individuals or groups *"vulnerable to disinformation"* then first you need to find them. Can you honestly think of a better way than by drawing them in to ostensibly benign activist organisations. From where they can be monitored, guided or used.

I am speculating and am in no way suggesting Zinc Network (Breakthrough) were knowingly engaged in such an operation. But when your client is a shadowy

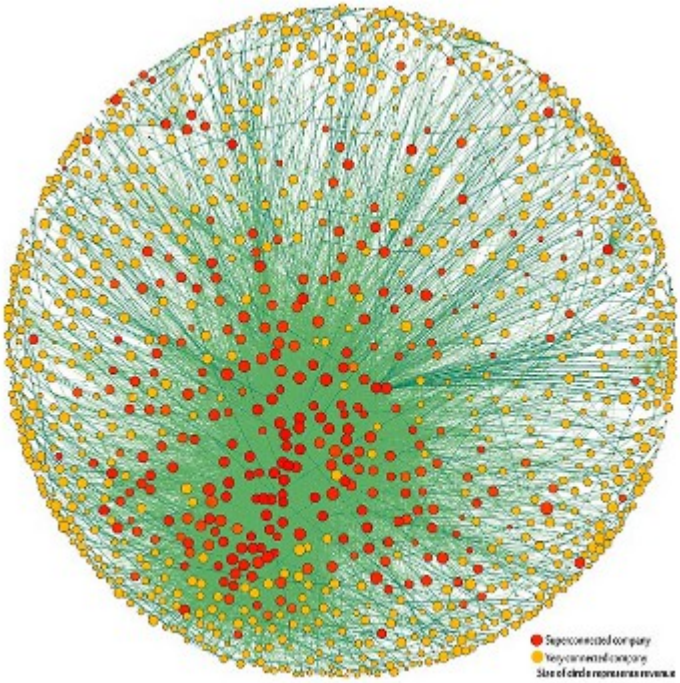
propaganda unit established by the Secret Intelligence Service, the possibility of your program, itself hardly open and transparent, being used, exists.

This method of embedding effective government agents inside media organisations and engaged citizen activist movements is precisely what the EXPOSE Network, led by Zinc Network and their partners, DFRLab, Bellincat and the Media Diverity Initiative has been set up to do. Everything we know about the EXPOSE Network indicates that it is not a *counter disinformation* organisation. It is on the front-line of a propaganda war devised nearly forty years ago.

The aim is not to undermine *Kremlin disinformation* which, on the whole, appears to present a relatively minor threat. It's target is not Russian troll farms, hacktivists or propaganda assets. It's target is foreign nation states, their popular media, western MSM outlets and our ability to openly and freely share information. It's aim is to provide the narratives that will shape public opinion over the coming years as the global corporate state moves towards its long dreamed of dominion.

Next, in the final part of the series, we will explore how the EXPOSE network is behind a much larger push for control of all information across Europe and beyond.

Chapter 7: the EXPOSE Network – The Full Picture



147 corporations control the global economy. Mapping the EXPOSE Network would look like this.

Over the previous five posts we have exposed the EXPOSE Network. To those who have read them, I thank you for your time. If you haven't, much of this post will prompt more questions than provide answers (hopefully).

In this concluding part we consider how, through a labyrinth of state initiatives, the EXPOSE Network sits within a cohesive, multinational, corporate & state run propaganda network. This is primarily a NATO/EU operation, led by the UK Government. Taking shape in 2018, it is obvious that Brexit has no impact upon

its development. We've explored NATO (and U.S.) critical involvement in the EXPOSE Network. This post is concerned with the European Union's.

When announcing the public facade of the EXPOSE Network, the Open Information Partnership, former UK Minister of State Alan Duncan stated:

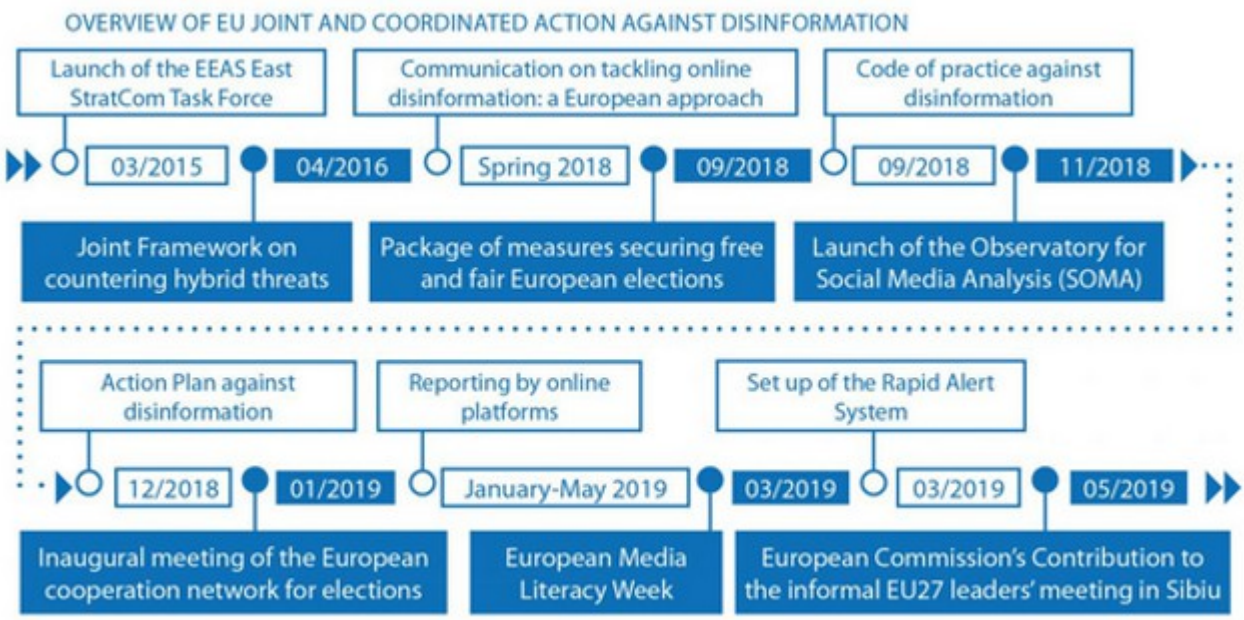
"We have a regular dialogue with international partners on the challenge posed by hostile state disinformation…….The Foreign Secretary (then Jeremy Hunt) discussed disinformation at the EU Foreign Affairs Council on 21 January in the context of the European Commission's ambitious Action Plan Against Disinformation…….by countering disinformation directed at the UK and its Allies from Russia…[with]..projects in a number of different countries that….. expose disinformation and share good practice with partner governments."

[Note: Bracketed information added]

The EXPOSE Network sits within "*the context of the European Commission's ambitious Action Plan Against Disinformation*." Duncan's statement alone is far from the only reason to believe this the case.

A few points are worth bearing in mind. Firstly the EXPOSE network targets mainly European nations, especially in Eastern Europe and the Balkans but also others in Central Eurasia, almost certainly with a view to expanding towards North & Central Africa and the Middle East. More precisely it targets both media coverage and news organisations in those nations in an attempt to influence their internal politics and international relations. The other objective is to control the West's perception and understanding of news events unfolding in these infiltrated sovereign states.

Secondly, all the suggested fear and panic about *Kremlin disinformation* is based upon very little, if any, credible evidence, as we shall see. Given the lack of evidence the only possible conclusions are either that the entire apparatus of the combined western state is run by idiots (possible but unlikely) or *Kremlin disinformation* is merely the cover story to obscure a covert operation. The latter being by far the most plausible.



The EU in Action

The EU Action Plan Against Disinformation, endorsed by the EU in December 2018, makes interesting reading. All of it is predicated upon the concept of hostile disinformation. Defined as:

"....verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm"

The meaning of public harm:

"…..includes threats to democratic processes as well as to public goods such as Union citizens' health, environment or security."

Once again, we see that definitions only *'include'* certain elements, meaning others exist. We just don't know what they are.

Much like the UK's Prevent Duty these woolly rationales appear to be designed to allow sufficient wriggle room for additional strictures to be applied, as and when required. Nor is a threat to democracy specified. Does this mean attempts to physically stop voters getting to the polls or does it equally apply to criticising electoral systems?

What is clear is that anything deemed a threat to public health or the U.N's Agenda 2030 Sustainable Development Goals will be considered *'disinformation.'* Again we are left in the dark to imagine what might constitute a threat. Though we can make an educated guess.

We have already explored the EXPOSE Network nexus between global corporations, governments, NGO's and wealthy *'donors.'* Vaccines currently represent a relatively small component of global pharmaceutical corporation's profits. In 2017 the global Vaccine market was conservatively estimated to be worth $34.3 billion annually. The projected Compound Annual Growth Rate (CAGR) was around 7%. However, recent moves towards compulsory vaccination has seen market confidence soar.

Agenda 2030: Criticism is verboten

With revenue projected to reach an estimated $77.1 billion per annum by 2024, an increased estimated CAGR of 10.3% is an attractive proposition for venture capitalists the world over. Especially at a time when EU Central Bank (ECB) interests rates have slipped to -0.5%. This growth is all but guaranteed providing as many people as possible are vaccinated.

Similarly, an offered 12% yield on tax payer subsidised Climate Bonds, with plans to create a market worth a projected $100 trillion, is even better. As long as people believe they are about to be killed by the plant food they breath out, and are consequently willing to stump up the required subsidies.

Safe to say, questioning vaccine efficacy will definitely be considered *'a threat to citizen's health'* and failing to jump on the climate emergency bandwagon will mark you out as *'a threat to the environment.'* In both cases you will be found

guilty of peddling *Kremlin disinformation.*

This Russian disinformation claim is the whole basis for the EU's wide-sweeping Internet regulations and the huge tax expenditure on STRATCOM operations.

It's All Evidence Based

We have also looked at the difficulty EXPOSE Network *'experts'*, such as DFRLab, have encountered when attempting to provide some evidence to back up their claims of a huge *Kremlin disinformation* operation. So, what is the EU's proof that Kremlin (Russian) disinformation is a real and present danger?

The EU Action Plan spells it out:

"The East Strategic Communications Task Force, has catalogued, analysed and put the spotlight on over 4,500 examples of disinformation by the Russian Federation, uncovering numerous disinformation narratives…."

East StratCom Task Force website

The Easta StratCom Task Force' (ESTF) main method for countering disinformation is *'raising awareness'* about it in their weekly *Disinformation Review.* The full record of the Task Force's work on disinformation is available on the ESTF's own EUvsDisinfo website.

The work of EUvsDisinfo is central to the EU Action Plan. It provides the evidence which informs the EU's assessment of the *Russian disinformation* threat. The influential U.S. think tank and policy advisors, the German Marshall Fund, wrote a policy paper in August 2019. They observed:

"EU vs Disinfo's research and documentation efforts were instrumental in changing the debate about Russian disinformation and hybrid threats within the European Parliament and EU institutions."

The *full record* of the 4,500 examples of disinformation, rather than emanating from academic or intelligence based assessments, are the sum of EUvsDisinfo's OSINT informed *'weekly reviews.'* For example their report on 24th October 2019 identified another 60 cases of *Russian disinformation.*

There were 12 cases of *'enemy of the west'* narratives, 7 about western moral decay, 5 alleging NATO war preparations, 10 saying the Ukraine is bad and 11 protesting Russian innocence. Only 45 in total, of which only 31 were linked to alleged evidence.

Given the ESTF are referenced by the EU as providing over 4,500 *hard evidence* examples of *Kremlin disinformation,* it would be helpful to see all 60. Otherwise, how can we trust the figures?

Clicking on any of the 31 contextual links, such as *"Neo-Nazis have outsized influence"* takes you to a page like this. In every case the *'evidence'* consists of allegedly identified Russian disinformation, called a *Summary.* The response, or *'Disproof,'* is then provided by an anonymous ESTF *'actor.'* You can also view the source of the Summary claim. In this case it's an episode of RT's "Cross Talk" political discussion program.

In order to *'Disproof' something, it has to exist in the first place.*

The observation that Neo Nazi's have an *"outsized influence"* was made during the program by Prof. Nicolai Petro, a professor of political science at the University of Rhode Island and a former special assistant to the U.S. State Department. He said:

"I would take a slightly different tack with respect to the right wing, neo-nazi element in Ukrainian politics. It exists, it has an outsized influence, but I don't really think it is the thing that is preventing change right now."

From this, the ESFT identified the following Kremlin disinformation:

"Recurring pro-Kremlin narrative casting Ukraine as a Nazi country."

At no point in the "Cross Talk" discussion does anyone cast the Ukraine as a Nazi country. The identified *'disinformation'* doesn't exist in the example given.

Another example is the link to crime infested no go zones where the ESTF identify the disinformation as:

"Recurring pro-Kremlin disinformation narrative linking migrants and asylum seekers in the EU to violent crime."

The ESTF quite rightly criticise RT for not citing the evidence to back up some of their claims. This is a common failing with the MSM. For example, when the UK Express newspaper wrote Europe's No Go Zones they only provided a couple of links. When the Canadian national newspaper , the National Post, wrote on the same subject, they too could have offered more evidence, as could the U.S based Fox News.

Regardless of their quality, what these articles demonstrate is that there is no evidence of the claimed *"pro-kremlin disinformation"* in the cited example. Unless the ESFT believe that pretty much the entire western MSM is *"pro-Kremlin."* I am not aware that they are.

Fox News. Pro Kremlin? I don't think so.

You can search the ESFT database referenced by the EU. Time and time again, when you check the links alleging Russian disinformation, proof either doesn't exist or is spuriously contrived from entirely subjective interpretations of mainly MSM content. Hard evidence, proving the scale of this fabled Russian disinformation operation, doesn't exist.

In March 2018 the ESFT were forced to issue a retraction after three Dutch media outlets threatened to sue them for falsely labeling them as *'disinformation.'* The ESFT acknowledged the Dutch were right and claimed they were *"taking steps to further improve."*

In fact, the ESFT don't seem to have much faith in their own investigations. Carefully adding a disclaimer to every *'Disproof'* stating:

"This does not necessarily imply, however, that a given outlet is linked to the

Kremlin or editorially pro-Kremlin, or that it has intentionally sought to disinform."

The EU. No evidence and nothing is implied. Just believe it!

Posing the question, if it implies that the story is neither linked to the Kremlin nor that it is pro-Kremlin and it doesn't seek to intentionally *'disinform'*, how can it possibly be '*Kremlin disinformation'*?

In the referenced example, there is no evidence that the East StratCom Task Force gathered 60 examples of Russian disinformation. They only cite 31 and none of those checked were substantive.

There is no reason to place any credence at all in the EU's assertion that, "*The East Strategic Communications Task Force, has catalogued, analysed and put the spotlight on over 4,500 examples of disinformation by the Russian Federation."*

The evidence, or rather lack of it, demonstrates otherwise. Admittedly I haven't trawled the whole database so perhaps there's some evidence, somewhere of

something. But it seems doubtful. At the very least, the EU need to revise their risible claim to *"over 4,440."*

As with the EXPOSE Network, it seems the EU's assertion, regarding the scale of Russian disinformation and the level of threat it presents, is fallacious. It is as if they are reading from the same script.

EXPOSE Network Drives The EU's Action Plan Against Disinformation

In March 2019 an open letter by European Security Experts to the President of the European Commission requested more money for the East StratCom Task Force (ESTF). Their current budget comes from the EU Strategic Communication fund of €5 million per annum. They are part of the European External Action Service (EEAS) who stand to benefit considerably over the coming years from a planned €123 billion investment.

EEAS – primary beneficiary of a €123 billion investment

Such a sizeable tax funded budget would be an enticing prospect for any non governmental organisation or private intelligence contractor looking for opportunities to improve their revenue stream. For example, a consortium of private contractor with all the necessary experience and skills might consider applying for a few billion euros.

One of EXPOSE Networks *'actors'* is the Institute for Public Affairs (Inštitút pre verejné otázky – IVO – named as prospective EXPOSE partners in the scoping document), based in Slovakia. They have confirmed their membership of the Open Information Partnership (OIP). Another appears to be the Union of Informed Citizens (UIC) working out of Armenia (also named in the scoping document). They recently received EU funding for *"taking initiative"* in *"information gathering."* As EXPOSE Network *'actors,'* they will be expected to report that information back to the Network Facilitator who will pass it on to the UK FCO and the CDMD.

The OIP web presence was created in order to give the EXPOSE Network a public air of respectability. The Zinc Network led consortium who form the Network Facilitator, based in the London Hub, described this in their technical proposal:

"*……..the Network needs to be public-facing…… the strategy for public facing communications is based on minimum requirements, such as a static website……..The project could expand to build on this public facing component, promoting the network as a journalist integrity and disinformation network…… Although the activities of specific Network Members will remain discrete……..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.*

This allows EXPOSE Network *'actors'* like the IVO and UIC, to manage their

reputations by openly declaring their membership of the OIP. These declarations should be seen as distinct from the Hub activity operated in London. OIP membership, in this context, indicates only that they are CDMD run EXPOSE Network assets, not Network Facilitators.

IVO are *'donor supported'* by the now familiar list of transatlantic funders such as NATO, the UNDP, the EU Commission, the NED, the Open Society Institute, the World Bank and so on, also enjoying wide support from a number of governments. As do the UIC.

We know that one of the EXPOSE Networks recommended *'fact checkers'* is the Ukrainian based StopFake. They report:

"Britain is thought to be leading [the] EU in building a grassroots campaign against Russia's attempts [disinformation]. The campaign is lead by the Foreign and Commonwealth Office and executed by a communications agency called Zinc Network."

[Note: Bracketed information added]

EXPOSE Network *'actor'* the European Values Center

Certainly when we look at the EXPOSE Networks *'actors',* that appears to be the case. Of these, perhaps one of the most influential is the European Values Center for Security Policy. Through them we can see how the transatlantic NATO/EU EXPOSE Network operates. Their two biggest funders are the Dutch government and the UK Foreign and Commonwealth Office.

One of their projects is called Kremlin Watch which claims to tell you *"everything you need to know about about Russian influence operations in Europe."* They also tell us quite a bit about the role of the EXPOSE Network in Europe. They state:

"Our team is the most active contributor to the EEAS East STRATCOM network (ESFT), which produces the Disinformation Review."

[Note: Bracketed information added]

It seems the EXPOSE Network is providing the *Russian disinformation* analysis, via the East StratCom Task Force, which the European Union are using to justify draconian Internet regulations and planned tax expenditure of €123 billion over five years. The quality of that analysis appears to be so poor we might consider if it is itself '*disinformation.*' The Action Plan builds upon the work of the ESTF, which is the work of the EXPOSE Network.

The EXPOSE Network is an operation of the Counter Disinformation and Media Development Program of the UK Government Foreign and Commonwealth Office (FCO). It appears the UK Government are working with the European Union to create a €123 billion tax payer funded budget based upon their own highly questionable *Kremlin disinformation* analysis. A healthy return on an initial £10 million investment. What really matters is that the tax paying public believe the threat is real.

The EXPOSE Network 'actor,' the European Values Center for Security Policy, proudly announces on their website the myriad of major MSM news outlets who have shared their work. The BBC, CNN, The Guardian, BILD, Time Magazine, the New York Times, Newsweek and others have all spread their, and now the EXPOSE Network's, message.

The EXPOSE Network's Amorphous Blob

As we discussed in Chapter 2, we cannot be certain about the name the EXPOSE Network is operating under, only that it exists and is operational. If your business is covert then exposure is the last thing you need. Perhaps this is why on the 01/11/2019 and again on 12/11/2019 Zinc Network filed to be struck of the companies register. However, just as they existed for 6 years, prior to registering as a limited company, under the Breakthrough Media umbrella. so their loss of separate company status means little. However it does mean, should Zinc Network continue to operate under that name, they won't be required to file official accounts.

Language can also present a problem when tracking EXPOSE Network players. For example OIP partners Fundacja Reporterów from Poland are listed in the FCO's EXPOSE Network scoping report. However, in English they are referred to as the Reporter's Foundation. For example on 1st November 2019 the Guardian wrote how the *Reporters Foundation* (Fundacja Reporterów) were a consortium of investigative reporters who sent an undercover reporter called Katarzyna Pruszkiewicz to work inside a Polish troll farm.

While there, Katarzyna discovered some shocking things. People creating fake profiles, writing social media posts undermining confidence in the Polish purchase of Lockheed Martin F35 fighter jet and so on. These detail were echoed in a report published in the Investigate Europe website on the same day. Three

days later Lisa Vaas, writing for the British Artificial Intelligence (A.I.) security software company Sophos, wrote almost the same article again. However, she also noted the *"alleged tactics resemble those used by Russia and its infamous troll factory."*

Linking to the allegations that Russia hacked the 2016 U.S. elections, using its *infamous troll factory*, Lisa was seemingly right to spot a common strand running through the Guardian, Investigative Europe, her own story and the Russian troll factory claims. She just picked the wrong one.

None of them are based upon any verifiable evidence. There are no social media posts cited by Katarzyna to backup her tale. Nothing the reader can check to verify any of the claims made. All we have regarding Pruszkiewicz' story is her word for it and all we have 'proving' Russian troll farm allegations are allegations.

Peter Pomerantsev, listed in the Zinc Consortium technical proposal as an *Independent Consultant*, was quoted in the Guardian article. Speaking about what all these unsubstantiated troll farm stories mean, he said:

"…..what it exposes is just how flimsy and ineffective our regulatory framework is."

Peter was *'lobbying to improve regulation'*. This is a requirement of EXPOSE Network members, as stated in the FCO's EXPOSE Network final scoping document.

There seems to be a lot of rebranding going on at the moment. Sut.am, a project of the Union of Informed Citizens UIC) in Armenia has just rebranded itself as the Fact Investigation Platform (FIP). They were listed in the EXPOSE Network

scoping document as Sut.am. As a subsidiary of the UIC (members of the OIP) it seems highly likely they remain involved. As they say on their own website:

"We would like to inform you that the website has been renamed. The change is related to our new branding policy. It does not imply a change in the activity and nature of the website. Fight against disinformation and fact-checking will continue to be the objectives of the website. Hereinafter SUT.am will have the new name Fact Investigation Platform."

What's in a name? StopFake, also listed in the FCO's scoping document, often publish the work of Roman Shutov calling him a journalist. Yet on his Facebook Page, he states he is also a Network Manager for the Open Information Partnership. Similarly Urve Eslas, listed in the the Zinc Network technical proposal as the Project Manager, calls herself a Network Manager for the Open Information Partnership.

The EXPOSE Network Fusion

Theresa May: – The Fusion Doctrine

The Fusion Doctrine is the enactment of the perpetual hybrid warfare proposed by Ronald Reagan nearly forty years ago. It deploys every sector of the state to fight the hybrid information war. In the 2018 National Security Capability Review (NSCR), then UK Prime Minister Theresa May wrote:

"….our national security is conditional……on our ability to mobilise most effectively the full range of our capabilities in concert to respond to the challenges we face…..we have agreed a new approach to the orchestration of our national security capabilities. Based on the new Fusion Doctrine…..Every part of our government and every one of our agencies has its part to play."

The NSCR later states:

"Our international approach has entered a new era……we are using our soft power to project our values and advance UK interests….The world has become more uncertain and volatile, we are committed to deploying the full suite of our security, economic and influence capabilities to protect and promote our security, economic and influence interests"

The Fusion Doctrine's *"whole of government approach"* represented a fundamental shift in the UK's governance structure. It centralised power considerably, placing far more in the hands of senior civil servants. Especially those within the Cabinet and Prime Minister's office.

The CDMD are funded via the Conflict, Security and Stability Fund (CSSF). Their CSSF budget allocation for the 2018/19 financial year was £20.1 Million in total, with £1 Million earmarked for Official Development Assistance (ODA) and £19.1 M allocated to Non-Official Development Assistance (Non-ODA). £2.7 M Of the Non-ODA was allocated to *"engaging with audiences potentially vulnerable to*

disinformation." This appears to be the bulk of the first year funding for the Network Facilitator of the EXPOSE Network.

In March 2019 the Independent Commission for Aid Impact (ICAI) issued a scathing report on the CSSF, finding it to be an opaque funding vehicle with unclear objectives, consequently unable to evidence effectiveness. It was noted that, since its inception in 2015, with annual budget of more than £1.3 billion, there was a risk that the CSSF was actually doing more harm than good. The report recommended:

"Programmes should demonstrate more clearly and carefully how they identify, manage and mitigate risks of doing harm."

Mark Sedwill – one man, a lot of power.

In their response to the ICAI, the UK government stated they were already working to remedy many of the highlighted problems. The CSSF works to

priorities set by the UK government's National Security Council (NSC.) The NSC are responsible for implementing the UK Strategic Defence and Security Review and the National Security Strategy that follows from it. Last reviewed in 2015.

Alex Aitken, the Executive Director for UK Government Communications and member of the UK National Security Council stated:

"Crucially, the Fusion Doctrine enshrines a place for strategic communications at the heart of national security issues……strategic communications are to be considered with the same seriousness as financial or military options."

While military and financial threats are observable, quantifying STRATCOM threats or *Kremlin disinformation* rely upon subjective analysis. This means, in order to secure funding for your SRATCOM project, all you really need to do is spin information and convince elected policy makers of the danger. If the threat doesn't exist, you can create it.

The NSC is largely a political body with various Cabinet Ministers and Committee members invited to join as appropriate, dependent upon the matter under discussion. The Chief of the Defence Staff and Heads of the Intelligence Agencies also attend when required.

The advisor to the NSC is the Permanent Secretaries Group chaired by the National Security Adviser, Mark Sedwill. He is also the current National Security Adviser to the Cabinet Office in addition to being the permanent secretary to the NSC, by virtue of being the head of the National Security Secretariat.

The EXPOSE Network, is a project of the CDMD, funded from the CSSF, which is set by the NSC. Ultimately it reports to the NSC and the National Security

Secretariat headed by Mark Sedwill.

How can we possibly sum up the EXPOSE Network?

The EXPOSE Network is a transatlantic full spectrum, hybrid warfare project. It is run by the UK Government Foreign and Commonwealth Office under the direction of the Counter Disinformation and Media Development Program. It reports the analysis of harvested data back to the National Security Council who control its official budget via the Conflict, Stability and Security Fund.

Its dual purpose is firstly to infiltrate, monitor and control the media of targeted nations in order to promote the economic, political and geostrategic objectives of NATO and the European Union. Secondly, it seeks to control the western media's news coverage of events for the same reason.

This is achieved by both control of information from its source and by manipulation of media reports via a network of embedded mainstream media journalists, infiltrated, coerced and controlled activists movements, cooperative Non governmental Organisations, global corporations, social media networks and

individuals. Using the false justification of counter disinformation, it seeks out, identifies, undermines and disparages any and all who question NATO/EU policy decisions or actions. Working in partnership with search engines and social media giants it relegates unapproved information to obscurity to hide it from the public.

Its resources are not limited to official budgets and direct political oversight is limited. It partners with a huge network of global interests each seeking, both individually and collectively, to benefit from the EXPOSE Network's capacity to influence NATO and EU policy. It is at the heart of the European Union's STRATCOM policy and uses manipulated information to mislead, misdirect and misinform both policy makers and public alike.

Its existence is anti democratic and its activities demonstrate total disregard for the principles citizens in western democracies hold dear. If it is all it claims to be then it should not fear scrutiny. It should be as open and transparent as it promises on its single page website and genuinely engage with the public's questions, born from the critical thinking it allegedly venerates.

Its is an immense threat to free speech and freedom of expression. Each an every one of us needs to exercise our rights, and demand the EXPOSE Network account for itself.

Well?