## New Approaches and the Way Forward in Strategic Communications

### Report from the conference StratCom Stockholm, 1 December 2017<sup>1</sup>

On 1 December 2017, the Swedish Institute of International Affairs (UI) hosted a closed workshop – "New Approaches and the Way Forward in Strategic Communications" – in Stockholm. The workshop aimed to explore and develop new local, national and international solutions for countering disinformation by bringing together key stakeholders, journalists and researchers from Europe and the United States. The workshop was part of a larger project on Strategic Communications sponsored by the Swedish Civil Contingencies Agency (MSB) in partnership with the Atlantic Council.

These proceedings provide a short overview of the discussions and highlight the main solutions and recommendations presented by conference participants.

### Aim and purpose

Disinformation has become a key tactic in Russia's efforts to win the information war against the West. "Fake news", targeted advertising and social media manipulation through bots, Russian attempts to shape the 2016 US presidential election are currently under investigation. Meanwhile, the Islamic State group has exploited disinformation, propaganda and strategic communication in order to legitimize, radicalize and recruit. Disinformation is also an internal threat in many Western countries. For instance, the current US president has spread fake videos and stories on Twitter and on multiple occasions labelled traditional media outlets such as CNN, the *Washington Post*, the *New York Times* and NBC "fake news" when reporting on the special counsel investigation into links between the Trump campaign and Russia during the 2016 presidential election.

Disinformation campaigns have also been targeted at simply eroding trust in general, exploiting societal divisions and sowing discord. These efforts have acutely highlighted how vulnerable Western societies and values are to disinformation operations and cyberwarfare. There is thus an obvious need for the USA and Europe to work together to come up with common solutions to counter these efforts. The UI workshop on 1 December 2017 aimed precisely to develop such solutions.

### Building Long-term Resilience: Local and National Perspectives

The first panel focused mainly on long-term solutions to disinformation at the local, regional and national levels. The panellists explained that there are many obstacles to building resilience against disinformation. Civil servants working at the municipal or regional levels often do not feel that disinformation is something that can or will

<sup>&</sup>lt;sup>1</sup> StratCom Stockholm was organized by the Europe Programme at the Swedish Institute of International Affairs (UI). For any inquiries, please contact Björn Fägersten, bjorn.fagersten@ui.se, Programme Director.

affect them – it is simply somebody else's problem. This is problematic as these levels were also identified as the "low hanging fruit" for spreaders of disinformation, not least since they deliver some of society's most critical societal infrastructure.

Participants also agreed that while there is a consensus about the destructive effect of disinformation, it is now crucial to go beyond identifying problems and start finding solutions. However, several speakers expressed concern about the lack of any academic consensus on what differentiates public diplomacy from propaganda. As public diplomacy efforts are being boosted in order to tackle disinformation, it is important to agree on the limits of these operations so that public trust in the state is not eroded. Agreeing on a definition of propagandistic content could also empower the public to identify disinformation on their own.

With regard to solutions, training for civil servants could be a practical and effective way of strengthening local resilience. Local and regional level communicators often express the need for a checklist on how to act during an adverse information operation, but they should instead be given the tools to think about the strategies that are being used and how they can be countered. It is thus only through education that we can build long-term resilience.

Another point that was raised is that we should treat disinformation in the same way as we address any other issue that requires a public information campaign. While we can tell society not to drink and drive or not to smoke, we should also shape behaviour in society to avoid spreading disinformation. Even if people want lies to be truths, we should not address disinformation any differently. However, this requires that the issue is addressed using all aspects of our democratic society.

The need to create a "modern psychological defence" was also expressed, specifically by identifying existing vulnerabilities in our societies and creating personalized (microtargeting) counter-strategies for different target groups, for instance by targeting younger people through social media instead of traditional media.

One argument was that the key to creating solutions that stand the test of time is to focus on and strengthen the values that underpin open societies, and to make society work for these values. If the aggressor wants to change our behaviour, we should focus not only on educating critical thinking, but also on making sure that the population knows what the best course of action is. In other words, in order to recreate a "defence will" within society, the role of the government is to empower bottom-up dialogue and engagement. Conversely, one panellist argued that governments should not just empower dialogue (and thus remain neutral), since there are some values that we should stand up for at all times. Society is not neutral against disinformation, and our actions to counter it should not be neutral either.

The discussion highlighted that long-term resilience is, by its nature, bottom-up. While some actions can be taken by the government, those actions should focus on transparency rather than banning. This will ensure that no "ideological dilemma" arises from the government's actions (i.e. internal propaganda). In addition, as solutions will always be imperfect, long-term resilience is rather about equipping the public with the tools to deal with the disinformation that does get through.

### What is the Form and Function of International Cooperation?

The second panel focused on new forms of international cooperation for countering disinformation. It was argued that a coordinated and networked response to disinformation is needed. One example is more coordination between the EU and NATO to respond to disinformation, for instance through joint training and exercising of EU and NATO communicators. This also means that any response to disinformation cannot be undertaken alone - for instance through spreading best practices or accurate information. Sharing information about what other countries do and what works well is highly effective which means dusting off the playbook and using our existing toolkit.

International cooperation is needed to counter all kinds of propaganda. This was a clear lesson from the migration crisis in 2015. It is essential that we now support local media and journalists in states with little resilience to disinformation (such countries in the Western Balkans) in order to foster a bottom-up approach and to help drown out Russian disinformation. In this context, it was suggested that the EU and NATO should cooperate on projecting 'forward resilience' - in a temporal as well as spatial manner. This could, for example, be achieved by increasing information sharing and considering dedicated advisory support teams to bolster foresight capacity and resilience in neighbouring states facing disruptive challenges to vital societal functions.

The need for continued dialogue and sharing of best practices was also highlighted. However, we should recognize that many of the practices that work well in Europe are not at all applicable to the USA. This is especially true with regard to internal sources of disinformation and trust in the government. While trust in government is high in Sweden, the same cannot be said of the Trump administration in the USA. We thus have to identify the best practices that are applicable in differing national contexts.

The EU needs to use its regulatory leverage to persuade social media companies to work against disinformation. If they wish to be part of the solution, they should also be part of an informal consulting group set up for discussions between governments, civil society and media companies. This consulting group could help to establish best practices and act as a forum for developing a voluntary code of conduct.

International cooperation is key, especially considering how complex the issue of disinformation is. Centres such as the European Centre of Excellence for countering hybrid threats in Helsinki and the Stratcom Centre of Excellence in Riga remind us of the risks of and solutions to disinformation campaigns. However, internal sources of disinformation can often do more harm than external, and they are much more difficult to handle. We also need to accept that we will never completely keep up with disinformation in the information space. However, we should not panic – we can live with the "gap" even if we can never close it.

The following discussion focused to a large degree on the role of social media companies in countering disinformation, for instance, how we should deal with companies that make money out of Russian disinformation through advertising revenues. One response from a technological perspective was that it is extremely hard to regulate disinformation, especially if that regulation is based on a notion of truth and

not the messenger. While content control is never the answer, transparency could be. It is not a threat to freedom of speech to identify the source or country promoting particular advertisements or articles, for instance by labelling countries that allow freedom of speech. However, attribution is difficult as it is now very easy to obfuscate the source of information online. An alternative solution could be fact checking. It is important, however, that such solutions are not rushed.

The last point made was that public service media outlets are perhaps not always part of the solution for countering disinformation. In some parts of the EU, for instance Poland and Hungary, the public service media is instead part of the problem. We should thus give increased recognition to private sector media as part of the solution.

# Fighting Back: Content and Technology to Counter Disinformation

The last panel of the conference mainly focused on the content of disinformation and the role of journalism, marketing and new technologies in countering it. The panellists had a diverse set of backgrounds, but in general agreed that the content of disinformation had evolved and become far more complex in just a few years. Back in 2014, fake news was easy to debunk by just googling it. Nowadays, "junk news", where most if not all of a story or an event is manipulated or staged, is regularly broadcast from Russia. While such events might have happened, the wider contexts are often faked. This makes the stories harder to debunk and, as a consequence, they are increasingly passed on by traditional media outlets as legitimate. The goal of this type of disinformation is mainly to confuse and distort logic and critical thinking in general so that people find it

harder to distinguish fact from fiction. Ultimately, the notion that nothing is true or correct leads to a distortion of some of our key values, such as human rights, democracy and freedom of speech. Russia is succeeding in this, and the tactics used are likely only to get more sophisticated in the future.

From a marketing perspective, advertising is more or less the same thing as disinformation - at least in terms of its methods. Both marketing and disinformation use information to evoke emotions. One key difference is accountability - if McDonalds lies in one of its adverts, claiming that burgers make us skinny or something similar, they can be sued. However, if Russia or some other source of disinformation spreads propaganda, it is much harder to demand accountability. Besides accountability, disinformation is also destructive by nature. Adverts make us believe that we need a product when in reality we might not, but they do not try to convince us to fear or hate each other, which is often the case with propaganda.

Another point made was that we already have most of the tools needed to combat disinformation - the question is simply why we are not using them. While it is important to share solutions and best practices with other sectors, we simply do not have the time to discuss what is fake and what is real news for another 25 years - all possible action to counter disinformation should (and must) happen now. In regard to solutions, there is a need to support a whole system approach. Education, workshops and systematic refuting of fake news can convince some of those in the "middle" of the disinformation spectrum - in other words, those who are about to switch from believing truth to believing disinformation (or vice versa). Such people can also be

micro-targeted by "dark ads" (optimized targeted advertising) in similar ways as they are used for disinformation and propaganda today. Money is a big issue when it comes to fake news (click bait leads to increased revenues), and the next level of technology will allow illegitimate adverts and fake stories to be filtered out. New ways of identifying legitimate sites and adverts using data forensics are constantly being produced, and should be further supported. From a corporate perspective, economic incentives were emphasized rather than legislative measures to get them on board this work.

Civil society was also raised as it should be increasingly mobilized to defend society against disinformation operations, in line with the reactivated concept of total defence, and stressing the whole-of-society approach. However, as shown above, the challenges are many. When asked about how they are preparing for disinformation in the 2018 Swedish parliamentary elections, one of the panellists expressed the need to actively raise awareness about the dangers of disinformation. One example that was highlighted was the nationwide effort to train all election officials at county boards and municipalities on how disinformation threats against the election can be countered. However, the final panellist concluded that he mainly prepares for 2018 by "praying to god". Unfortunately, that succinctly summarized the mammoth task that we have ahead of us.

### Key recommendations by conference participants

- Train and educate local and regional level civil servants and communicators on how to identify and counter disinformation.
- Treat disinformation in the same way as any other issue that requires a public information campaign.
- Identify existing societal vulnerabilities and personalize counter-strategies for different target groups.
- Make the population work for the values that underpin an open society by empowering bottom-up dialogue and engagement.
- Be transparent about efforts to combat disinformation.
- Coordinate, network and cooperate as much as possible with other states.
- Project 'forward resilience' by offering targeted support to neighbouring countries.
- Share best practices and support forums for cooperation such as the Helsinki CoE.
- Work to create a voluntary code of conduct on disinformation for social media companies, as well as economic incentives for the corporate sector to engage.
- Apply a whole of system and society approach to countering disinformation. Education and systematic refuting of fake news can help to persuade those who are on the "edge" of believing disinformation.
- Mobilize civil society in defending democracy against disinformation.