SOCIAL MEDIA'S ROLE IN 'HYBRID STRATEGIES'

AUTHOR: THOMAS ELKJER NISSEN

PREPARED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

INTRODUCTION

Hybrid Warfare seems to be the new buzz word, like asymmetric conflict and counter-insurgency have been before in connection with Iraq and Afghanistan, when it comes to describing the activities that Russia allegedly carries out in Ukraine, including the annexation of Crimea, and towards the Baltic States, Georgia and Moldova to name a few. There is, however, a difference. Unlike Russia, different non-state actors cannot to the same extent use diplomatic, economic, media, cultural and social activities, coordinated with the actions of special services and Special Forces, in an orchestrated way in order to exert influence. Non-state actors therefore fight in an asymmetric way, but they do not employ ‘hybrid strategies’ – while Russia does. If we are to call it hybrid warfare that is because Russia doesn’t. Russia accuses the ‘West’ of conducting hybrid warfare and information attacks against Russia, not the other way around. Russia, on the other hand wages ‘New Generation Warfare’ or ‘Non-linear Warfare’, but even those terms are not precise, although their purpose is.

The purpose is to create doubts and mistrust towards the western media and the political ‘elite’, slowing down decision-making processes through media and diplomacy, affecting the unity and cohesion of alliances (including attempting to play countries out against each other), covering up real objectives and, not the least, affecting civil society and its perceptions, beliefs and behaviours, in the countries in question.

This is achieved by supporting and facilitating different communication activities, including a variety of activities in the political, cultural, civil society, media and cyber domains. These can cover everything from the creation of front organisations (in the form of for example NGOs and other forms of ‘single-interest’ organisations) to the use of ‘agents of influence’ to so called ‘patriotic hacktivism’. A common denominator that these activities aim at affecting the information environment in and around the targeted countries, public and media discourse and, in turn, political decision-making.

Understanding the information environment, and the role media, in particularly social media, plays in it, also helps one to understand some of the mechanisms, techniques and methodologies brought into play by different actors (state or non-state) in order to affect civil society. This happens in ’peace-time‘ long before actual hostility is recognized as anything other than an element of the ever on-going debate or political discourse in a liberal democracy.

Understanding the techniques brought into play also helps to recognise these kinds of activities, to determine what to do about them and how best to create societal ‘resilience’. Before looking at the role of social media in these kinds of activities, we need to discuss how civil society and its information environment can be influenced both overtly and covertly.

‘INFLUENCING’ CIVIL SOCIETY?

Influence activities are primarily carried out in ‘peace-time’ before violence or hostilities occur, in order to shape the public, media and political discourse. Influence, in this context, is the systematic application of informational and other means by a state or non-state actor to clandestinely undermine or overthrow a liberal democratic government or an international organisation, fomenting civil strife in the interest of this actor. The activities are predominantly aimed at weakening (shaping) a country’s political, economic, social, cultural, scientific, technological and military structures in order to exert the desired influence. This influence can be aimed at either a contextual change or a behavioural change in society and in the political discourse and subsequent decision-making. A contextual change would basically mean the overthrow of a government leading to a regime change, which potentially could lead to the formation of new alliances and a review of memberships of international organisations and ratifications of international agreements, conventions, laws and treaties. This change doesn’t necessarily have to be violent, it can simply be a question of influencing elections or international negotiations. A behavioural change would mean that the current government or regime stays in power, but significantly changes its policies in a way that supports the actor´s strategic objectives. For example, this could be done on the basis of perceived attitudes in the electorate – brought about though influencing the media and public discourse. The common denominator is that communications play a vital part in the activities.

INFLUENCE ACTIVITIES CAN HAVE MANY FORMS AND MAY BE HARD TO DETECT

Activities aim at exploiting the vulnerable parts of civil society (foremost in liberal democracies). They target the natural vulnerabilities that are part of a social structure based on democratic values and principles. The activities can exploit the freedoms of the press, religion and speech, and the natural divisions in society (ideologically, ethnically, by religion and language) that result from these freedoms. They can also exploit (at least perceived) contentious topics in the public discourse, such as a democracy deficit, social policies on education, language, immigration and rights of certain minorities, corruption, priorities in foreign policy, or historical grievances. They can address topics which have the potential to divide particular segments of society and motivate some to act in a particular manner – be that politically or otherwise. Influence activities can, however, also exploit issues with existing laws and other forms of legislation and matters that are not codified or regulated. Influence activities can, therefore, target the "inner system" of a nation. The actors, most likely, will try to stay "formless" in order to escape detection and thereby avoid mitigation by a country's police, security services and government. They will also avoid becoming an issue for debate in the media, risking exposure as influence activities.

Many of these influence activities build on principles such as non-attribution, creation of an 'information fog' and the projection of a particular narrative in order to, primarily clandestinely, shape or frame issues in the public discourse and political decision-making. Non-attribution is about not having any clear links between the information outlets, the information itself and the persons, or personas (for example fake profiles on social media), using them and the state or actor behind them.[1] This is to create confusion as to what really is going on by using selected pieces of information, contradictions, fabrications, misleading information and outright lies. This makes the audience unable to tell what is right and wrong in the information environment and creates leeway for alternate narratives and framings of specific events – both current and historical. Influence activities are targeted at many functions and areas of civil society and include, but are not limited to; political (including economic), civil society, cultural, media and cyber activities.

POLITICAL ACTIVITIES

Political activities include orchestrating political events, demonstrations, civil disturbance and general unrest, by exploiting existing laws in the target nation. Political influence activities can also involve financial support to opposition parties (opposed to the current government or its policies) and lobbying activities aiming at changing laws and regulation in a way favourable for the foreign power. Conversely, it can also entail exploiting existing laws for political gains, for example, by filing complaints against the state, state institutions and /or individual political decision-makers (to be subsequently used in media activities).

CIVIL SOCIETY ACTIVITIES

These can include creating and supporting both government-organized non-governmental organizations (GONGOs) and NGOs or 'single-issue' political interest organisations to work within civil society with the aim to influence the public discourse and deliver tangible evidence of actual support for a cause. It can also be a question of supporting and promoting ex-patriate communities (based on language or ethnicity, for example), friendship organisations or fake grass-root organisations. The latter is also known as 'astroturfing' (fake grass-root organisations). Finally, it can be about influencing conversations in the public domain at gatherings, meetings and public lectures and conferences. Civil society activities can therefore range from rather obvious activities supporting NGOs affiliated with the aims and objectives of a foreign power to covert activities aimed at injecting a foreign power's themes and messages into civil society.

CULTURE AS A MEANS FOR INFLUENCE

Cultural activities can involve arranging or supporting specific sports events and different kinds of competitions on language, culture and history, sometimes in order to frame and interpret historical events and concepts. This can also involve attempts to give existing symbols new meaning and re-frame the meaning of them, or to distribute new symbols (for example ribbons to wear in connection with specific dates and events). Finally, cultural activities can also involve the exploitation of religion and religious institutions as authoritative voices, either to make messages resonate or to emotionally entrap audiences.

THE ROLE OF MEDIA

Media activities are focused on either of two main goals - securing control over the information dissemination infrastructure by direct ownership or indirect control of the editorial process, or through content placement by many different means. Often it can be a combination of the two. With respect to media infrastructure, it can involve buying up media outlets (exploiting ownership laws), creating one's own news outlets or news agencies, or through intimidation of media owners or employees. It can also involve subsidizing existing opposition media, either overtly and/or through dummy owners or NGOs. The primary purpose is to secure influence over the editorial process and decisions.

With regard to content, influence activities mostly involve creating credibility and a sense that the sources being are independent. In order to achieve this, media activities in support of influence activities can involve creating apparently independent 'think-tanks' or research institutions. These can provide content in the form of policy analysis, fake academic reports that can bring other research into question, or rephrase it, and produce polling results based on manipulated questions and or statistics in order to frame news coverage of current events.

The use of experts in the media to interpret events, influencing or discrediting other experts used by the media, or through intimidation of such experts, can also be a part of media activities. Here, 'agents of influence', can be brought into play. Agents of influence are normally associated with persons using their official or public position to exert influence on policy, public opinion, the course of particular events and the activity of political organisations or state organs in a target country. Agents of influence are generally citizens of the country targeted for influence activities who are controlled by a foreign intelligence service. These agents are not perceived by the general public as being tools of a foreign power. Their purpose is to influence public discourse on specific topics by inserting specific phrases and concepts into the public discourse that serve the foreign power's interests. Unlike 'agents of influence', so-called 'useful idiots' are advocates on their own initiative for a cause that serves the outside power, who are not fully aware of the ultimate goals of the cause and are cynically used by the foreign power. They are often approached and supported by front organizations which cannot be linked to a foreign power.

A part of media activities is also the creation of specific products and content that is favourable to the foreign power, but not associated with it or attributed to it. This can entail the support to and production of books and booklets, TV-documentaries and movies (for sale or for free) and the publication of op-eds and articles in news outlets or on blogging sites. These products will be published under pseudonyms or aliases, by front organizations or even in by using names of known public figures without their consent.

THE INCREASING ROLE OF THE CYBER DOMAIN

Cyber activities are the last of the five main activities. In a modern information environment, environment, these are, naturally, closely linked to media activities. Cyber activities can be divided into two categories – technical activities and informational content.

The technical activities entail Distributed Denial of Service (DDoS) attacks, defacing websites, leaking e-mails and tapping mobile phones . They can also include hacking of news-outlets to either hinder access to specific stories and information, or to use collected information as user-generated content in other media-outlets later.

With regard to content as a cyber-activity, "trolling" is probably most talked about. Trolling includes the use of fake social media accounts, bot-nets, and aggregation of information sources to create a particular picture of current events or manipulation of audio-visual material and other user-generated content that can also be a part of influence activities.

'Social engineering' also plays an increasing role. Trolls and social engineering will be discussed below.

INFLUENCE IN AND THROUGH SOCIAL MEDIA

With the increasing role of cyberspace, social media has become an integral part of the conflict environment over the last 15 years. It started with what has been called the first "internet-war", the Kosovo conflict in 1999, and the development has been steadily evolving ever since. Social media have been used more and more strategically by multiple state and non-state actors to create effects in both the virtual and physical domains. Some examples are the counter-insurgency campaigns in Afghanistan and Iraq, several conflicts between Israel and its Arab neighbours, particularly Hamas in the Gaza strip and Hezbollah in Lebanon, the events in connection with the Arab awakening (or spring) and several 'colour revolutions'. This has been especially noticeable during NATO's operations in Libya, the ongoing civil war in Syria, the latest events in Ukraine, and the pressure put on the Baltic States and NATO/EU partnering nations as Georgia and Moldova.

Most conflicts for western liberal democracies today are so- called "wars of choice", requiring a high degree of legitimacy. For multiple non-state actors struggling to mobilize support and to find new ways of fighting asymmetrically, social media seems to have become a weapon of choice. Social media are easy for nearly every actor to access and use, due to the democratisation of technology, facilitated by developments in information and communication technology. It creates effects disproptionate to the level of investment. In other words, using social media to achieve desired effects gives you a high return on your investment. These effects support the goals and objectives of the multiple actors "fighting" in the social media sphere, and include influencing perceptions of events, which, in turn, affects decision-making and the behaviours of relevant actors, as discussed above. Due to the global connectivity that social media provides, the actors are no longer just the direct participants to the conflict. They can be whomever (states, non-state actors, civilians and activists) desires to achieve an effect. Therefore the terms "remote warfare" and "social warfare" play an increasing role in contemporary conflicts, where social media is now used for political and military activities such as, but not limited to, intelligence collection, targeting, propaganda and disinformation, offensive and defensive operations and command and control activities. This stratification of social media and the effects achievable by using them, including the empowering and re-distributive effect on international power relations and diplomacy, has affected the character of contemporary conflicts. Another consequence is that target audience can be everyone from states to individual citizens. The latter are becoming increasingly targeted through social media.

Obviously social media therefore play a role in all of the five main influence activities discussed earlier. The activities conducted in, and through, social media can occur under cover of being a part of the 'democratic debate' in any given country. As with influence in general, activities carried out in social media, and also more broadly in digital media, can contribute to the creation of controversy over public policies and help create civic strife in the interest of a foreign power by influencing and shaping the conversations and debates within all aspects of civil society. This doesn't necessary have to happen only in connection with a political debate on defence and security issues, but can also be involve with more benign topics as sports and culture where a foreign power can have an interest in shaping the conversation. This can, for example, involve on-line rumour-campaigns about symbols and historical or current events. Or it can simply be a question of circulating multiple different stories or narratives about a given event in social media network to confuse audiences as to which one is the true one and thereby undermine the credibility of other actors' narratives. Social media can also be used to mobilize people for political activities, such as demonstrations, on-line lobbying for or against the adaptation of new laws, exposing illegal activities or simply insinuating that they are happening. Social media can therefore also be a very useful tool for GONGOs and NGOs both in order to establish themselves and to get into the public discourse, but also to help create a perception of them having 'mass', among other things, by what is known as 'social engineering'.

This can result more radical ideas being seemingly 'normalised'. People in the large group of 'uncommitted' might feel confident expressing themselves believing that many of their perceived 'peers' do the same, in effect becoming 'useful idiots' for a given cause themselves. The effect of social engineering can also be multiplied through the use of technologies as 'bot-nets'. Social engineering, however, can also be much more targeted at specific individuals or groups of people – through social media.

SOCIAL ENGINEERING

One of the challenges with using social media networks for different types of influence activities against civil society is that it requires that you to gain access to networks that might otherwise be closed. In order to gain this access, one needs information or intelligence about the networks and the persons in them and their interests, preferences, their access and status within the networks. In other words, you need intelligence in order to 'target' networks and individuals which you would like to influence. To this end social engineering is used to gain access to otherwise closed networks.

Social engineering is a blend of science, psychology and art. While it is amazing and complex, it is also very simple. Basically, it refers to psychological manipulation of people into performing actions or divulging confidential information. In other words it is about influencing a person to take an action that may or may not be in their best interests. It is, therefore, a type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. The term "social engineering" as an act of psychological manipulation is associated with social sciences' (e.g. psychology, marketing, communication etc.), but its usage has caught on among computer and information security professionals as well, as it has become more and more widespread in social media.

Regardless of the social media platform, users are fooled online by persons claiming to be somebody else. Unlike the physical world, individuals can misrepresent everything about themselves while they communicate online, ranging not only from their names and business affiliations (something that is fairly easy to do in-person as well), but extending as well to their gender, age, and location (identifiers that are far more difficult to fake in-person). Initially an actor can be simply 'trawling' a network to see how is there and who reacts, after which a more targeted approach is taken and a target is contacted. Trawling can be simple 'phishing' – sending out spam e-mails or SMS with some sort of encouragement to react. More sophisticated methods involve 'spear-phishing' and 'whaling', where the e-mail or SMS to tailored to individual recipient. The contact (particularly in the case of whaling) will be based on some sort of 'pretext'. In other words, a reason for the 'target' to engage with the actor (this can be a perceived common interest, for example). The actor has often identified this common interest based on what the target itself has published on-line on his/her social media profiles, but can also be combined with 'real-life' data collection. This pretext is then used to model the communication leading to the elicitation of some sort of behaviour (e.g. giving the actor access to one's network for example) allowing the actor to further map one's network for other potential targets and to disseminate information.

The social engineering process therefore consists of several steps, ranging from information (intelligence) gathering and subsequent 'social network analysis' to personality profiling. In addition, some sort of contact will be established based on the identified pretext. After that, the actual 'attack' or influence activity will be conducted. Sometimes there will also be an 'exit' or dis-engagement phase involved.

Once you have access, through social engineering, you can perform two important functions: further intelligence gathering and (targeted) influence activities. Not everything, however, is linked to closed social networks. Quite a bit also goes on in more open social media networks and platforms.

OUTSIDE CLOSED NETWORKS

Access can be used to influence conversations through the delivery of content in social media and digital media in general. This can be either in the form of actual messaging, or through offering links to reports, use of graphic materials (often very emotional) or references to news articles or blogs supporting a specific claim or interpretation of events. To this end, so-called trolls or agents of influence are probably the most commonly used techniques. Hence, the typical profile of an agent of influence on-line is a person who appears to be an 'independent' researcher (scientist), writer or perhaps journalist. They all have reasonably free hands in regard to what they can express themselves about and can lend some credibility from their public profession.

In theory social media can therefore by used for, or in support of, nearly all forms of influence activities and most predominantly as a playground for "agents of influence" using cross-media communication techniques offering opportunities to identify and cultivate "useful idiots". Most interestingly, social media provides actors with amble opportunities for 'social engineering' based on some sort of pretext. At the end of the day, influence activities will therefore most likely be done through both open and closed sources and networks simultaneously, making it hard to detect and mitigate.

DETECTING INFLUENCE AND DECEPTION IN SOCIAL MEDIA

The use of social media for influence is, however, based on the accumulated effect of multiple (often un-attributable) indicators, signals and messages in the digital information environment, not one dominant single voice or source, and is therefore also difficult to detect. For starters one has to look for any re-representation of arguments and messages outside relatively small social media "echo-chambers" or networks and for any signs of this activity leading to actual off-line behaviour supporting it. Can you, however, taken the relative "formless" state of these activities into account actually say that it is a result of targeted or planed influence activity, or if it just a part of an expected public debate in a civil society?

Deception-detection (e.g. the identification of for example fake profiles, false content and or content attribution and pinching of identity information and attempts of social engineering) is, based on the tools and techniques described above, therefore a very challenging issue for all actors. As discussed earlier the use of botnets and sock puppets and different ways of hiding your true identity on-line makes it very difficult to detect and attribute false messaging in social media networks. This has also led to numerous government and academic studies into how to detect deception on amongst other platforms Twitter, but also in general how to detect 'trolls' and attempts of social engineering.

One such study looking into this issue was conducted at Georgia Tech School of Public Policy and it found that there are four characteristic on-line behaviours of twitter 'hyper-advocates'. Firstly they are sending high numbers of tweets over short time periods. Secondly they are re-tweeting while themselves publishing little original content. Thirdly they quickly re-tweeting other´s content, and fourthly they are coordinating with other, seemingly unrelated accounts, to duplicate, or near-duplicate, messages on the same topic simultaneous.(1) Another study by the Canadian SecDev Group points to another set indicators on on-line deception that amongst others include that shortened URLs in tweets appears differently but lead to the same URL (example a specific news story or press-release). There is also little interaction with other twitter accounts, all posted links refer to the same two or three news outlets and the central account don´t follow other accounts. The relaying (re-tweeting) accounts follow most of the same accounts, having the same tweeting and re-tweeting behaviour over a 24 hours period and generating thousands of hash-tags (#) based on the same three letters.(2) Also the US Department of Defense research institute DARPA (Defence Advanced Research Projects Agency) have a programme called "Social Media in Strategic Communication" that amongst other things look at detection of deception and misinformation in social media.(3) All three studies suggest, though, that examining on-line behaviour not content in order to detect deception is most important. Besides that is trying to identify clusters of ‘users’, having the same or similar political ‘ideologies’, whose aim is to create an ‘echo-chamber’ to increase perceived legitimacy of an actor or other source and amplify some issues and minimise others also is a way of identifying online deception.

Other studies conducted in Poland and Latvia looks at the identification and classification of trolls and trolling activity, and how to mitigate these activities, as it will also be discussed in some of the subsequent chapters in this report.

(Endnotes)

[1] Michael Terrazas: Four Telltale Signs of Propaganda on Twitter. May 31, 2012. http://www.scs.gatech.edu/content/four-telltale-signs-propaganda-twitter.

[2] SecDev Group: Syria Cyber Watch. Published on-line 25 November 2012. www.secdev.com, page 2.

[3] DARPA http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx.

CONCLUSION

Strategically, influence is generally aimed at undermining the stability of a society (in peace time) in order to create conditions that can lead to change, either contextually or behavioural, which is brought about by a combination of activities both overt and covert. Often very emotional and or controversial issues and topics are used, drawing on events (historical or current) that are already known to the audience. But also some events are orchestrated and substantiated with fictional events, fake persons (sometimes actors), non-existing academic sources, conspiracy theories and contradictions. All is done in order to create the desired effects. These effects are often associated with uncertainty and mistrust towards the existing establishment (media and political elite) and fear for the future (mobilizing a particular behaviour).

The activities are exploit societal vulnerabilities and legislation. The activities themselves are generally un-attributable to any specific actor and stay under the threshold for what can be regarded as aggression or an ‘attack’. The activities are often small and subtle, and conducted along multiple “lines of operation” (e.g. the five main influence activities), and it is the long term accumulated effect that matters. But most importantly, the predominant parts of ‘peace-time’ influence build on ‘communication’. Communication that to a higher and higher degree is based on, or carried out through, social media.

In the context of hybrid strategies or non-linear warfare, social and other forms of online media play a large role in attempts to influence people’s perception of current events and topics. Much of the activity in social media in this context is deceptive in nature, utilising both direct and indirect approaches to content creation and placement, among other things, social engineering and trolling. Most methods, though, tend to be indirect, as it is hard to distinguish between ‘persons’ and ‘personas’ online, or between real and fake social media profiles. The latter are extensively used for ‘social engineering’ through either one person operating multiple personas or through the use of bot-nets to the same end. Regardless of the technique employed, it aims at manipulating the public discourse in, and through, social media. It is, however, not only in the social media domain the effects occurs. In many instances social media are used as intermediate platforms in order to get content into the traditional news-media, further obscuring the real source of the information. Whether technical or human, one of the most talked about techniques in the current propaganda struggle, over among other things Ukraine, is trolling in different shapes and forms. But it is not the only technique employed, and it is getting increasingly hard to detect and mitigate influence and deception online, as these activities are carried out within all aspects of modern ‘online’ civil society, not just within the defence and security domain.

This article is a product of the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does not represent the opinions or policies of NATO or NATO StratCom COE. The views presented in the articles are those of the authors alone.

Photo: David Mallett, Flickr