

I am going to start of reading a few excerpts from a government document.

*Psychological warfare utilizes a certain situation and adapts its methods to its circumstances. Propaganda cannot manufacture new attitudes and expectations out of thin air. It must play on those needs and attitudes already in existence within the audience.*

*Collection of information regarding the political state in a country, the existence of frustration and tension between different groups are important inputs directing the design of propaganda. Manipulating words and expressions is a common methodology. Using words that are emotionally charged, positively or negatively, in new contexts. Opponents are labelled "fascists" or "warmongers" and sympathizers are "progressive". Those who resist are "aggressors".*

*In totalitarian states today ... convincing the population plays a key role. The modern version of such states carefully frame legislation and elections to make it seem as if the citizenry is fully behind every decision.*

These text excerpts were not written to describe recent events. These words are from the 1952 government inquiry that started the formation of the Swedish "Emergency Response Board for Psychological Defence".

In this day and age it is easy to get swept away in specific alarming examples: bots, dark ads, data collection of 87 million Facebook accounts and the decreased barriers of entry for conspiracy theorists, fringe groups and state influence operatives alike. Indeed new technology and channels of communications are important to understand and consider, but it is beneficial to remember that influence methodologies, vulnerabilities, even actors and their strategic aims are rarely completely new occurrences.

As an analyst it is easy, when contemplating the current information climate, to get lured into a pessimistic outlook. Sweden is, as other western democracies, faced with new channels and technologies that have benefited adversarial and populist messaging, as well as groups that feel their time has come, some of which not only have an anti-democratic agenda but in addition a proven propensity for violence and actively build international networks. This also makes them well positioned to conduct subversive activities or otherwise act as proxies for hostile state actors.

Simultaneously, we have a security environment in the Baltic Sea region which has worsened as of late. An area in which Sweden is positioned

strategically from a geographic and thereby defence-related standpoint. There are also, as in many other countries societal challenges to consider. Migration flows and integration, urbanization, police and defence forces needing to adapt and grow in response to new demands, the outsourcing vulnerabilities related to key data and infrastructure and maintaining a high level of healthcare and education for all citizens regardless of where they live in our country.

Perceived cracks in the "contract" between the citizen and government institutions can act as fertile ground for influence from other states as well as domestic groups. Such actors can paint these challenges into society wide doomsday scenarios, blame a "liberal elite" and "mainstream media" to polarize our society and make it more difficult to govern, or market "traditional values" that just so happen to be bundled with an ideal of more authoritarian types of governance. This type of messaging is also spread in other countries about Sweden to denigrate the perception of our country aiming to make collaboration with other democratic states and alliances more difficult.

But, in terms of resilience to challenges in the information environment, we must also consider positive potential. In the latest Economist democracy index Sweden scores third of 167 countries. The World Value Survey shows that Sweden is one of the nations with the highest levels of interpersonal and social trust globally. A trust that recurring Swedish studies have found to be very stable over the last 30 years. Credibility of especially public service and leading newspaper media sources is also comparatively high in Sweden, with slightly lower numbers for the young adult demographic and those with right wing political sympathies.

The increasing international tensions as of late have exposed how the use of different capabilities aimed at the information environment can be a threat to democratic societies. The Ukrainian crisis and recent elections in the US and France have highlighted how a combination of intelligence-, computer network- and influence operations can be used in synergy to complement each other. The Cambridge Analytica case has also shown the immense opportunities for data collection and the psychographic targeting it enables.

Looking at the US election 2016, we can draw some conclusions about the aims and methods that can be employed to influence:

1. Denigrate the credibility for the election process through disinformation or hacking targeting election related systems.

2. Influence the will and capability of citizens to cast their vote
3. Influence political preferences through hacks and leaks, micro targeted ads, trolls and botnets
4. Influence the public perception of targeted politicians and officials

Sweden, however, is very different than the US in many respects, and time has passed so awareness is up and the element of surprise is gone. Lessons learned can therefore be informative, but a carbon copy approach to preparedness should be avoided. From my vantage point, if we are looking at a state actor conducting influence against our upcoming election, the primary aim will likely not be to directly affect the election results, but rather ensure that whichever parties form the next government will have a decreased capability to project a strong domestic and foreign policy, on our own or with other likeminded nations.

We must also remember to avoid getting stuck in a singular focus on our upcoming election - the underlying motivations fuelling the use of influence techniques are generally long term in nature. An election is indeed a situation where a lot of debate happens within a society, credibility can be won or lost and key decisions are made that can affect our country for years to come. But from an influence operative perspective, that is just one link in a longer chain of opportunities and stratagems.

When considering how to counter influence related threats it seems logical at first to focus on the actors orchestrating such campaigns as well as the methods and channels they utilize. The dilemma with this approach is that you risk drowning in a myriad of blips on your radar. In Sweden, we have chosen to instead build a situational awareness by focusing on our own information environment. Since attribution has become increasingly difficult due to new channels of dissemination we start with identified areas of societal vulnerabilities, a process already in use for our national crisis management, build a baseline and follow actions that are aimed at exploiting them.

Since we have a system of independent state agencies with different responsibilities collaboration becomes key. Civil contingencies, intelligence, military, police and the government offices all have different sensor, analysis and counter capabilities to contribute to a joint effort. Connected to this, clear strategic communication and transparency is also an important way to be proactive and ensure that our citizens receive information from credible sources in the early stages of a situation.

One of the challenges during the last US presidential election was that a broad awareness of the threats and vulnerabilities was lacking. Hence, even though irregularities were observed by different institutions, and local officials, the building blocks enabling joint analysis and action were not in place at the time.

We must therefore attempt to bridge that divide. Such resources in western democracies have traditionally developed occupational-specific approaches, systems and cultures. Aspects relating to these different skillsets are also often debated separately and in different societal forums. This needs to change if we are to increase our long term resiliency as well as our more immediate response capabilities.