DEN NORSKE ATLANTERHAVSKOMITE

THE NORWEGIAN ATLANTIC COMITTEE

Security Policy Library 2-2017

CYBERED INFLUENCE OPERATIONS: TOWARDS A SCIENTIFIC RESEARCH AGENDA

Lior Tabansky

Fridtjof Nansens plass 8, N-0160 Oslo–Tel: 22 40 36 00–Fax: 22 40 36 10–E-mail: post@atlanterhavskomiteen.no

In this contribution, **Lior Tabansky** offers a unique insight into strategic cybersecurity, facilitated by his over 15 years' experience in the professional IT-sector, his Political Science & Security Studies knowledge (PhD 2017), think-tank research experience, and his cyber strategy expertise for various corporations and governments.

Lior holds a Master of Arts in Security Studies from Tel Aviv University, where he also recently finished his PhD. His master's thesis, "The Role of Advanced Technology in Israel's Struggle Against Palestinian Terrorism, 2000 to 2005", earned critical acclaim and ignited public debate. Tabansky's book from 2015, *Cybersecurity in Israel*, co-authored with Professor Isaac Ben-Israel, is the first comprehensive "insider" account of decades of Israeli policy and operations. Moreover, the book develops an original analysis of the roles that grand strategy and innovation play in cybersecurity.

Tabansky's doctoral dissertation, "Explaining National Cyber Insecurity: A New Strategic Defense Adaptation Analytical Framework" (2017), explains why even the most developed nations remain so exposed to destructive cyber-attacks on strategic homeland targets by foreign states. It includes a comparative analysis of critical infrastructure protection and national strategy of Singapore, Israel, and the United States.

Published by: The Norwegian Atlantic Comittee
Editor: Magnus Vestby Thorsen
Printed by: Heglands AS, Flekkefjord
ISSN: 0802-6602

For more information, visit our website: www.dnak.org

Cybered Influence Operations: towards a scientific research agenda

Lior Tabansky

Abstract
Cyberspace in general and Social Media in particular provide new and affordable tools for actors to pursue their interests. The risk of hostile Influence Operations leveraging cyberspace to shape and manipulate public opinion, political debate, and decision-making is no longer theoretical. The Nordics, Baltics, Central and Eastern European countries devoted much attention to pro-Russian cybered Influence Operations for years, long before the 2014 seizing of Crimea. European threat perception in general, and cybersecurity view in particular, shifted drastically towards information warfare. The 2016 U.S. presidential elections, allegedly meddled by similar hostile cybered Influence Operations, brought global public attention to the topic.

Is information manipulation an unseen source of 'softer' power that Russia skillfully exploits? If that is the case, will Western democracies suffer fast-increasing public discontent, ill-informed decision-making, and unraveling of EU and Euro-Atlantic ties? The overestimation of the threat, which elicits inappropriate and counterproductive defense policies that undermine basic liberties – is the major alternative risk.

Science lags behind the fast-changing reality of cybered societies: we lack valid means to assess cybered influence effects and societal vulnerability. Science indeed suggests that Influence Operations via Social Media could produce extensive effects *en masse*, stronger and faster than ever. Moreover, empirical findings support assertions that Russia conducts intensive hostile cybered Influence Operations through the use of Social Media, to manipulate public opinion, decision making, and electoral processes in many European democracies.

However, estimates of the hostile Influence Operations power are entirely speculative. No reliable measurement of effectiveness of the recent hostile Influence Operations via Social Media has been

made public by the affected nations. To the best of my knowledge, reliable measurement was not even attempted. Therefore, we simply don't know whether hostile cybered Influence Operations using Social Media produce the feared political effects, what their extent is, and let alone, the causal mechanisms. This paper lays the agenda for cooperative interdisciplinary research to advance international security in the age of cybered conflict.

Acknowledgment: The Blavatnik Interdisciplinary Cyber Research Centre (ICRC) at Tel Aviv University (TAU) supported this research in their 2014 exploratory grant.

The science of power

According to Joseph Samuel Nye, Jr., one of the most influential international relations scholars and a former chairman of the US National Intelligence Council, power is the ability to affect others to obtain the outcomes you want. Nye distinguished hard and soft power along a spectrum from command to co-option in a seminal 1990 article.[1] One can affect the behavior of others in three main ways: threats of coercion ("sticks"); inducements or payments ("carrots"); and attraction that makes others want what you want.[2] Hard power relies on coercion and payment, while soft power uses the framing of agendas, attraction, or persuasion. Nye also discussed cyber power, masterfully including both physical and informational instruments, soft and hard power aspects, and ramifications within and beyond cyberspace.[3] Manipulation of information may, in principle, assist each type of hard and soft power. Since most of the worlds' information is digitally produced, processed, stored, and transmitted, cyber power is - '…the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power'[4] - intertwined with information.[5]

In recent years, Europe, and the U.S. after the 2016 elections, devotes much attention to pro-Russian cybered Influence Operations as a national security threat.[6] The common threat scenario that Western defense thinkers depict is usually along these lines: Russia will achieve its strategic objectives by exercising massive sustained influence on public opinion, leaders' preferences, and democratic political processes in the

1 NYE, J. S. 1990. Soft power. *Foreign policy*, 153-171.

2 Ibid.

3 NYE, J. S. 2010. *Cyber Power*, Belfer Center for Science and International Affairs; Harvard Kennedy School.

4 KUEHL, D. T. 2009. Cyberspace and Cyberpower. *In:* KRAMER, F. D., STARR, S. H. & WENTZ, L. K. (eds.) *Cyberpower and national security.* National Defense University Press : Potomac Books.

5 NYE, J. S. 2010. *Cyber Power*, Belfer Center for Science and International Affairs; Harvard Kennedy School.

6 GILES, K. 2016b. Russia's 'new' tools for confronting the west : continuity and innovation in Moscow's exercise of power. *In:* RUSSIA & EURASIA, P. (eds.). London: The Royal Institute of International Affairs Chatham House. EXCELLENCE, N. S. C. C. O., SVETOKA, S. & REYNOLDS, A. 2016. Social media as a tool of hybrid warfare.

West by daringly exploiting the new information-communication infrastructure, in concert with other more traditional means.[7]

I have researched this drastic shift in Europe since 2013, while situated outside the theatre of operations in Israel's TAU ICRC.[8] Observing from a distance, I developed an independent analytical perspective. Is information manipulation an unseen source of softer power that Russia skillfully exploits? Or, are Western defenses misled by the hype? How do cybered Influence Operations fit in with theories of power and international security? More practically, what should Western defense do regarding Russian cybered Influence Operations? The answers to these questions will drive far-reaching operational and strategic results. We better answer these questions by focusing on a clear fact-based understanding of reality.

How then should we improve our understanding? While social activity cannot be reduced to Newtonian laws of mechanics, science remains the greatest foundation of progress. The essence of science, the demarcation between science and pseudo-science as developed by Karl Popper, is the scientific method: science puts theories to rigorous tests, seeking to refute – rather than verify – the theory. Popper's falsificationist methodology offers a clear criterion that distinguishes scientific theories from metaphysical or mythological claims.[9] When theories are falsified by observations, scientists can either respond by revising the theory, or by rejecting the theory in favor of a rival, or by maintaining the theory as is and changing an auxiliary hypothesis. In either case, this process must aim at the production of new, falsifiable predictions. Science evolves by falsifying theories with observations and selecting against them.[10] Notwithstanding Thomas Kuhn's seminal contribution,[11] demonstrating how

7 In January 2014, NATO set up a Strategic Communications Centre of Excellence in Riga as a direct consequence of the Russian information-warfare campaign.

8 Tel Aviv University - Blavatnik Interdisciplinary Cyber Research Center.

9 POPPER, K. R. 1965. *The logic of scientific discovery,* New York, Harper & Row.

10 POPPER, K. R. 1972. *Objective knowledge : an evolutionary approach,* Oxford, The Clarendon Press.

11 KUHN, T. S. 1962. *The structure of scientific revoutions,* Chicago, The University of Chicago Press.

science communities actually work to defend the established paradigms, Popper's scientific method remains logically valid. Scientific hypotheses must be falsifiable by some possible empirical observation or logical statement (Popper called these the hypothesis' potential falsifiers). Scientists must sincerely attempt such falsifications on a regular basis.

Applying the scientific method to the situation, Western defense concerns should be stated as a multi-stage hypothesis:

a) **Cybered influence is a potent source and instrument of power**
b) **Russia employs hostile cybered influence as an instrument of international conflict, targeting democratic political processes in numerous Western societies**
c) **Russia's cybered influence operations seriously threaten core Western interests**

This paper develops a conceptual framework to advance international security by providing scientific foundation for Western defense and cybersecurity policy. I proceed by testing the three elements of the hypothesis.

Is cybered influence a potent source and instrument of power?

This section introduces several issues for research regarding Influence Operations via Social Media. The idea of undermining the adversary within his own country in concealed ways is an ancient and inherent part of all strategy and conflict.[12] Research on social influence is interdisciplinary with roots in many disciplines, including Social Psychology, Neurosciences, Communication, Political Sciences, Sociology, Business Marketing, Economics, and Computer and Information Sciences. The original research was built on explicit or implicit models of tight and bounded communities. Most of us have some experience influencing or failing to influence people in these types of relationships. Transportation, mass media, and telecommunications expanded the spatial reach of social connections well before the Internet.

12 MURRAY, W. & MANSOOR, P. R. 2012. *Hybrid warfare: fighting complex opponents from the ancient world to the present*, Cambridge University Press.

With Internet and Social Media, influence is no longer one person being influenced by mass communication or one person influencing another one-to-one. Rather, the impact of network size, strong ties, mutual awareness, socially similar (homophilous) network members, geographical and social proximity, clusters of ties, bridges across clusters, and how people navigate among clusters in their complex networks, change the equation. The general consensus is that online social media must have significant effects on the information ecosystem and its use. More research is needed in all these fields – and indeed much progress is already reaching maturity. In the current paper, I focus on the following: The fundamentals of influence, and two recent researches on cybered influence.

Influence: the gap between attitude and behavior

All information campaigns and Influence Operations presume causal relations: disseminated information alters attitudes of recipients, which then changes people's behavior and action. Influence process can result in two distinct types of outcomes, of increasing significance:

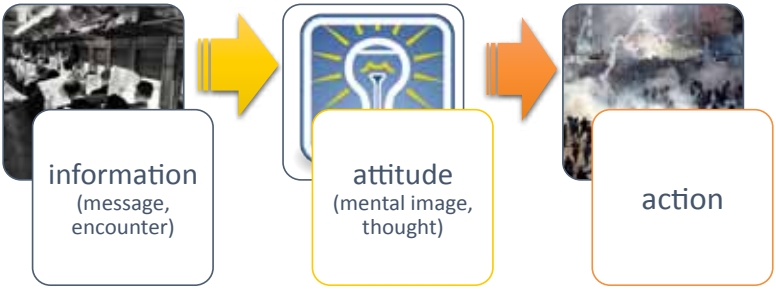

Figure 1: Influence process and outcomes.

However, much of the debate on influence simply implies that attitude change causes behavior change. In fact, already 80 years ago it was established that even overtly and voluntary stated attitudes are very poor predictors of behavior. Richard LaPiere of Stanford University conducted the first social psychology field study of racial behaviors, measuring real-life incidents and thus providing external validity. For empirical investigation of the national sentiments regarding non-Caucasian individuals at the

time, LaPiere traveled across the 1930s USA by car with a couple of Chinese ethnicity.[13] In the course of two years, they visited 251 hotels and restaurants; only once in their 66 hotel stays were they refused lodging and they were never refused service in the 184 restaurants in which the couple ate. Six months after his trips, LaPiere mailed questionnaires to 251 hotels and restaurants that they had visited. The establishment owners were asked: 'Will you accept members of the Chinese race as guests in your establishment?' Over 90% (i.e. 92% of those who were asked the question per se and 91% of those whose question also was paired with other nationalities such as Germans, Armenians, Italians and the like) of the 128 respondents (81 restaurants and 47 hotels) indicated that they would not. Other than one respondent who indicated yes, the remaining respondents indicated that they were uncertain, depending on the circumstances. LaPiere match paired control establishments that had *not* been previously visited by the couple, sending them questionnaires, finding a similar 92% 'no' response. In sum, LaPiere showed that questionnaires to measure prejudice and discrimination were poor predictors of how individuals actually behaved to real-life people.

The 1934 article Attitudes vs. Actions was seminal in establishing the gap between attitudes and behaviors.[14] Nevertheless, people often tend to extrapolate from attitude to action, including in current crucial policy and security realms. Consider the debates on:

- Social integration of migrants of different religious or ethnic background
- Public politics of sexual minorities
- The relation between far-right political attitudes and violent political behavior

How do Social Media change influence operations?

Information Communications Technologies are used to create, process and transmit information at an unprecedented enormous volume, with a global reach in real time, at near-zero cost. Unlike top-down TV or radio, the Internet and the

13 LAPIERE, R. T. 1934. Attitudes vs. Actions. *Social Forces,* 13**,** 230-237.
14 Ibid.

WWW provide new two-way (or many-to-many) channels for cheap, mobile, bottom-up, interactive communication via text, sound, images, videos and live streaming. At minimum, the Internet and especially online social media platforms facilitate many-to-many, one-to-many, and many-to-one types of communication, on scale impossible by traditional means.

Non-exclusive categories of social networks on the internet, 2017
Instant messengers (IM) including VoIP: (WhatsApp, Telegram, Signal, Skype, Viber, Facebook)
Online social networks: (Instagram, Snapchat, Facebook, LinkedIn, Twitter)
Email including address books: bidirectional and asynchronous way of communication (Gmail, Mail.ru, outlook.com)
Dating (Tinder, OKCupid,)
Media sharing (Flickr, YouTube)
Commerce and payment (PayPal, EBay, WebMoney, AliPay)
Massive multiplayer online games (World of Warcraft, Steam)

Looking at the above list, this 2008 quote is illustrative in what it omits:

"User-generated content—and a sort of collective intelligence—has become one of the dynamic and influential aspects of cyberspace via capabilities such as blogs and Wiki sites."[15]

The human communication landscape has dramatically changed. Facebook was launched in early 2004; YouTube beginning in 2005; Twitter emerged in the mid-2006; WhatsApp in 2009; Instagram in 2010; and Snapchat in 2011.

Since January 2012 to January 2017, more than 1,3 billion people started using online social media – a rise of 88% in just five years.[16] That translates to almost 1 million new users each day, or more than 10 new users every second. Mobile social media users have grown by more than 50% in two years since January 2015 – 13 new users every second. Online social media are a dominant force:

15 Kramer, F. D. and L. K. Wentz (2008). Cyber influence and international security. Washington, D.C., Center for Technology and National Security Policy, National Defense University. Page 61.

16 https://thenextweb.com/insider/2017/03/06/the-incredible-growth-of-the-internet-over-the-past-five-years-explained-in-detail

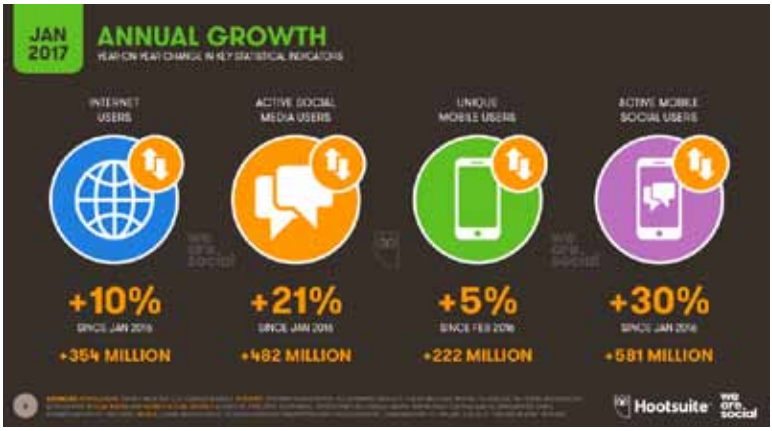

Figure 2. [17]

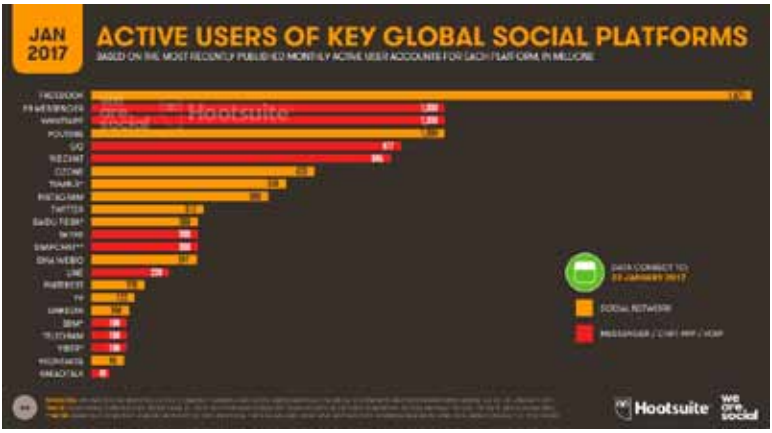

Figure 3: Active users of social media platforms.

Target Audience Analysis (TAA)

The advent of Social Media has not only increased the accessibility of the global information infrastructure. To achieve effect, a message must fit the audience. Adopting a scientific approach for influence and persuasion, it is useful to conceptualize a process in which the actor attempts to influence target audience (TA). Typical Target Audiences are:

17 https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2017/01/Slide008.png

- Leaders, decision-makers
- Trusted Communicators (family, friends, newspaper editors, TV anchors)
- Influencers: knowledgeable, favorable, local messengers[18]
- Demographic sets: geographic area, gender, age, ethnicity, occupation, education, political affiliation, religion, language, socioeconomic status
- Groups sharing common interests: social, professional, hobby, sport

The primary actors, or ultimate target audiences, are the people that will perform the desired behavior. Secondary actors are the "individuals or groups that have the ability to directly or indirectly influence the behavior of the primary actors."[19] While the discussion of Target Audience Analysis (TAA) exceeds the scope of this article, it is essential to realize that Web use and Social Media enable unprecedentedly effective ways to identify groups and individuals to micro-target them with custom messaging. Online Social Media created an environment which helps to target messaging more precisely by orders of magnitude. Online influence is big business today with many mature companies offering services designed to measure, increase, and effectively utilize influence. Although most are not explicitly political, they potentially boost political influence online. Social Media allows for micro-targeting, thus increasing the chance of effective campaigns. Facebook knows and provides excellent data for advertisers. Moreover, other traces can be extremely useful in establishing identity.[20] In addition to companies, state-sponsored cybered influence campaigns to alter populations behaviour (typically regarding public health or social norms) have become the norm rather than the exception.

18 Malcolm Gladwell describes different types of influential messengers: mavens, who validate the message; connectors, who link different parties and groups; and salesmen, who are effective at marketing. GLADWELL, M. 2002. *The tipping point : how little things can make a big difference,* Boston, Back Bay Books.

19 2007. Field Manual FM 3–05.301 *In:* ARMY, D. O. T. (ed.) *Psychological Operations Tactics, Techniques, and Procedures.* p. 2-4.

20 MAYER, J., MUTCHLER, P. & MITCHELL, J. C. 2016. Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences,* 113**,** 5536-5541, DE MONTJOYE, Y.-A., RADAELLI, L., SINGH, V. K. & PENTLAND, A. S. 2015. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science,* 347**,** 536-539. LUCAS, E. 2015. *Cyberphobia: identity, trust, security and the Internet*, Bloomsbury Publishing.

Hostile state-sponsored cybered influence campaigns do not operate in a vacuum. It is easy to make your ideas available online for anyone to see. But, will your target audience find these ideas among the sea of information available online? We must carefully support state-sponsored influence operations, and avoid baseless scaremongering.

Voter mobilization

The entire Western political thought since ancient Greece cautions that democracy depends on citizens' participation. But, in Western democracies, a substantial amount of citizens choose not to exercise their right to influence their government. Decades of political science research demonstrate that voter turnout in all national and local elections steadily declines. In recent US midterm elections, typical voter turnout is below 40%. The majority of citizens do not bother to exercise their most powerful tool as citizens.

Multiple efforts to mobilize citizens to vote, from fundamental school education to economic incentives to bombardment of party campaigning, have been largely ineffective. In parallel, political science electoral studies demonstrates that a very small change in voter participation is enough to swing the results of a competitive election.

The prestigious scientific journal *Nature* published a letter in 2012, "A 61-million-person experiment in social influence and political mobilization".[21] The authors test the hypothesis that political behavior can spread through an online social network with a randomized controlled trial of political mobilization messages. One of the researchers is a data scientist working for Facebook corporation. The scientists used this circumstance to design an extraordinary large-scale experiment: **61 million** users of at least 18 years of age in the United States who accessed the Facebook website on the day of the US congressional elections. About 60 million users (98%) received a 'social message', which included the same elements but also showed the profile pictures of up to six

21 Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489, no. 7415 (09/13/print 2012): 295-98. doi:10.1038/nature11421

randomly selected Facebook friends who had clicked the 'I voted' button. About 611,000 users (1%) received an 'informational message' at the top of their news feeds, which encouraged them to vote, provided a link to information on local polling places and included a clickable 'I voted' button and a counter of Facebook users who had clicked it. The remaining 1% of users were assigned to a control group that received no message.[22]

The social message group (N = 60,055,176) was shown a statement at the top of their 'News Feed'. This message encouraged the user to vote, provided a link to find local polling places, showed a clickable button reading 'I Voted', showed a counter indicating how many other Facebook users had previously reported voting, and displayed up to six small randomly selected 'profile pictures' of the user's Facebook friends who had already clicked the 'I Voted' button.

The informational message group (N = 611,044) was shown entirely identical message, poll information, counter and button, with one exception: they were *not shown any faces of friends*. The control group (N = 613,096) did not receive any message at the top of their News Feed.

The researchers compared the groups' online behaviors, and matched 6.3 million users with publicly available voting records. The experiment showed that the online social network quadruples the effect of the single Facebook social message. Seeing faces of friends - peer influence and digital social signals - significantly contributed to the overall effect of the Social Media-delivered message on real-world political behavior.

The researchers estimated that the social message directly increased turnout by about 60,000 voters, and indirectly through social contagion by another 280,000 voters, for a total of 340,000 additional voters. That represents about 0.14% of the voting age population of about 236 million in 2010. But the appropriate comparison for the 0.34 million would be with the 85 million actually exercising their right to vote, not the total 236 million. It is thus possible that more of the 0.60% growth in turnout between 2006 and 2010 might have been caused by a single message on

22 https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401

Figure 4: The messages delivered in the experiment.

Facebook. Moreover, turnout among those who received the informational message was identical to turnout among those in the control group, suggesting that *information alone* has no effect on real-world political behavior.

To summarize:

1. Online messages might influence "real world" behavior. Political mobilization works in online social networks. It induces political self-expression and information gathering, but also validated voter turnout.
2. Social mobilization in online networks is significantly more effective than informational mobilization alone. Showing familiar faces to users can dramatically improve the effectiveness of a mobilization message.
3. "Weak ties" are, well, weak. Online mobilization works when it spreads through strong-tie networks. Close friends exerted about four times more influence on the total number of validated voters mobilized than the message itself.

Content creation and distribution

The audience not only consumes, but also produces and distributes its own content. The current ability to massively create and communicate not just text, but sounds, images, and videos means that textual analysis alone is insufficient to understand communication. With improvements in artificial intelligence applications to voice, graphics and video, the skilled human Photoshop expert will no longer be the cost of entry to the game.[23]

In social networks, information shared by friends and acquaintances seems more credible than the same message coming from elsewhere. With increasing accountability risks of sanctions in Facebook, Twitter and websites, WhatsApp groups has become the key mechanisms of spreading questionable content, rumors and conspiracies. Simply captioning a real video or an image (e.g. a car in a traffic accident) can drastically shift the perception. But the source of the content is often misinterpreted, if a known person has shared it. An interesting psychological mechanism is the increased sense of trustworthiness when friends are in the process. Overall, social media coupled with software-driven automation (including bots and artificial intelligence) offer unprecedented ways to boost message design, delivery, engagement, assessment, all at a very low cost.

This changed the environment for influence and persuasion drastically. The global technological infrastructure – including the Internet, mobile devices, Social Media platforms, geopositioning, media creating and editing software, machine translation, big data analytics, chatbots, botnets, organized cybercrime groups and so forth – allows all sorts of actors to leverage these capabilities. But our experience of influencing, using cybered technology within and across social groupings, is short. Consequently, the functions of influence in social technologies are scientifically underdeveloped. In Western networked societies, it is easy to claim influence, but not as easy to exercise influence.

23 https://www.economist.com/blogs/economist-explains/2017/07economist-explains-3

a)	increase the volume of information delivered through diverse direct communication channels and messengers through genuine users or bots (including peer-to-peer)
b)	increase the level of targeting. Social Media platforms allow to segment the target audiences into dozens and thousands of subgroups for unprecedented ability to know your audience (Target Audience Analysis (TAA))
c)	Taylor personalized custom messages, timing and delivery channels for each target audience
d)	Communicate with videos, images and sounds to leap effectiveness: “facts speak louder than words” and ”picture is worth a thousand words”
e)	Identify influencers, trend-setters, opinion leaders (including via statistical means)
f)	Create the impression of credible source (including peer-to-peer relay; altered or misrepresented multimedia; user-generated content or bots; cyberattacks)
g)	Create engagement via participation (including share, reply, like, hashtag)
h)	Leverage existing context in real time to trigger message delivery and message design

Resilience to cybered Influence Operations

Any Influence Operation is just one part in the information overload and “noise.” Influencing American children to eat their vegetables, influencing citizens to go vote, and influencing your boss to allocate budget for a new armchair, clearly require different strategies. Even though the cybered operating environment is the same - context is crucial for influencing. Hostile Influence Operations are substantially different from domestic traditional political and commercial marketing and advertising, thus facing higher inherent obstacles. Translating communication into influence when messages originate from outside the target’s culture is even more complicated by substantial controversy, language and culture.

- Language: It is well established that audience will resist messages that appear non-genuine. People almost instinctively sense even minor mistakes in language use. While Russia Today and Sputnik News have done admirably in establishing broadcasting in many European languages, difficulties will remain. It is interesting to note that the Hamas viral videos

attempting to intimidate the Israelis have been met with total public ridicule.[24] One major reason was the heavy accent in Hebrew, another is the amateurish video production level. On the other hand, Daesh video propaganda is much more difficult to laugh at.[25] Can we reasonably assume that outsiders will perfectly craft the messages in a long clandestine campaign?

- Cultural differences: The targeted state, the population at large with elected officials, government servants, and other leaders, are divided along racial, cultural, religious, linguistic, economic and other lines. In the business world, a foreign company seeking to enter another country's market usually secures the guidance and support of local partners, joint ventures, and advisors – and often all three. Hostile Influence Operations need local partners; in fact, many RT "experts" can be considered as such. Outsiders lack understanding of tacit cultural differences. To exemplify, just consider yourself living outside the major cities in a European country other than your own. Can we reasonably assume that all the local norms and preferences are identical to those in the capital?

- The explosiveness of the issues: The attacker seeks controversial and subversive aims. The desired result is principally different from shifting consumer choice from McDonalds to Burger King, or from political competition amongst legitimate candidates within a sovereign legal framework. Can we reasonably assume that the mechanisms of influence, audience susceptibility, and engagement are similar between consumer advertisement and deep value-based issues?

Can educated people effectively assess information without gatekeepers?

Rulers, societies, and people have relied on gatekeepers – national broadcasters, accredited reporters, publishers, editors, and subject matter experts – to vet the information they consumed. "It's in the news!" remains an instinctive claim for reliability.

24 https://en.wikipedia.org/wiki/Shock_Israel%27s_Security

25 2014. *Visual propaganda and extremism in the online environment,* Carlisle, Pennsylvania, Stategic Studies Institute, United States Army War College Press.

Online Social Media circumvent the entire system we have built for centuries. Perhaps "Digital natives", widely presumed to be much better equipped to deal with online information than older generations, can spot and resist blatant falsehoods? The results of the study ending in June 2016 refute this assumption.

The Stanford History Education Group has prototyped, field tested, and validated a bank of assessments that tap civic online reasoning: the ability to judge the credibility of information that floods young people's smartphones and computers.[26] The target audience, high school students, are "digital natives" who spend hours each day online, both as consumers and creators of information. Consider the following photograph that the researchers presented for evaluation.

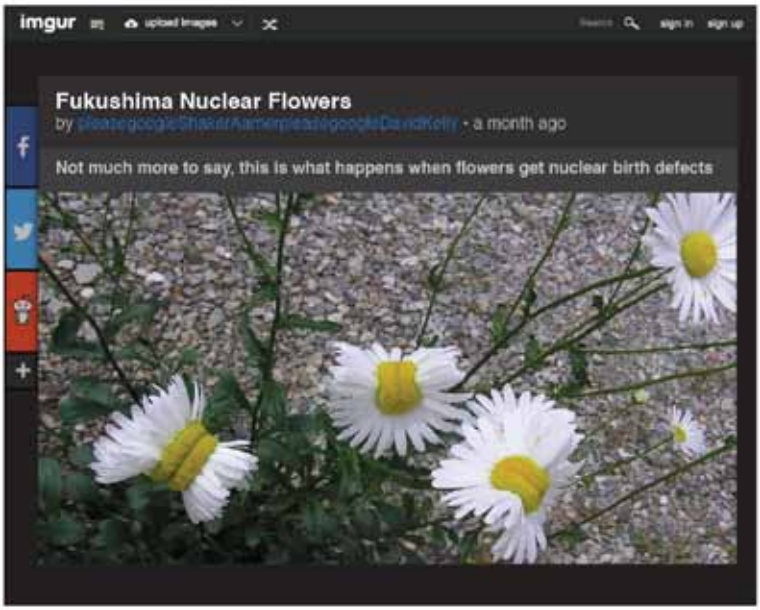

Figure 5. From The Stanford History Education Group experiment.

26 WINEBURG, S., MCGREW, S., BREAKSTONE, J. & ORTEGA, T. 2016. Evaluating Information: The Cornerstone of Civic Online Reasoning. Stanford university.

The title and the caption for the strange daisies claim that the flowers have "nuclear birth defects" from Japan's Fukushima Daiichi nuclear disaster. Students may question the credentials of the person who posted this photo to a site where anyone can upload and caption any photo. Students may question the image authenticity, seeking proof that the picture was indeed taken near Fukushima after the nuclear disaster. Students may rely on their prior knowledge: do daises grow in Japan at all? Are Japanese and American daisies identical? Students may question the logic: assuming the photo is real, was it nuclear radiation that caused the unusual daisies? Almost none did. The context is important. The website imgur is a free photo sharing service: anyone can upload and share any type of image, anytime, from any source. No authentication of users, captions, sources is required. Digital natives know that as they are often experts in generating and sharing customized images and videos. Digital natives know that today's smartphones have brought much of the capabilities of professional graphic designer and video editor to the user. Overall, at each level - middle school, high school, and college - young people's ability to reason about the information on the Internet can be summed up in one word: bleak.[27] There is no valid reason to assume that even the best-prepared citizens will invest the minimal effort to judge the credibility of information.

What is Russia doing, and why?

The theoretical aspects discussed above set up the framework to analyse empirical evidence on Russia's operations, goals and strategy.

"The Lisa case"

Disinformation, propaganda, and influence campaigns supporting Russian interests have been evident in many EU member states at least since 2013. NATO adopted "the Lisa case" as the template of Russian influence operations. For the first time, different Russian coordinated elements of influence were identified by Western experts. Germany saw a record influx of 1.1 million migrants from the Middle East in 2015, which intensified debate on immigration as well as protest marches by the *Patriotic Europeans against*

27 WINEBURG, S., MCGREW, S., BREAKSTONE, J. & ORTEGA, T. 2016. Evaluating Information: The Cornerstone of Civic Online Reasoning. Stanford university.

the Islamisation of the West (Pegida) movement. In Cologne New Year celebration on 31.12.2015, some 1,000 young men arrived in gangs to the cathedral square and railway station, and sexually assaulted and robbed numerous German women who went to celebrate. The scale of the crimes suggests some planning and organization, and highlights the weakness of German law enforcement agencies. Despite multiple reports on online Social Media, public and commercial German traditional media avoided covering the events until four days later.[28] This further fueled conspiracy theories that the "elites" and "lying press" cover up inconvenient truth even at the cost of harm to citizens.[29] The phrase "Rapefugees not welcome" was coined by right-wing demonstrators as a slogan following the events in Cologne.

This context is crucial to understand in "the Lisa case" – but it rarely appears in articles discussing it. On January 11, a 13-year-old Russian-German girl with dual citizenship from Berlin-Marzahn, that went to school in Berlin, had gone missing. The incident was circulated in real time in the large Russian-German (*Deutschlandrussen*) Berlin community and with online social media. She returned after 30 hours and told her parents that she had been abducted by three unknown men of "southern" or "Arab" origin, who did not speak German well. Furthermore, she initially told the police that she had been beaten and raped.

The German police established that she had been with a friend that night. Several days later, the Berlin correspondent of First Russian TV ran the news story suggesting that the Russian girl had been abducted and raped by several migrants – but German authorities was covering up the case for political reasons. Russian foreign media like RT, Sputnik, and RT Deutsch reported on the case. Social media, as well as rightwing groups, propelled the information on the internet. Small demonstrations of Deutschlandrussen as well as neo-Nazis were organized via Facebook, amongst others in front of the Bundeskanzleramt in Berlin on 23 January. Russian foreign media in Germany reported from these demonstrations, which brought it to the German mainstream media and to global news. The story dominated the

28 http://www.spiegel.de/international/germany/cologne-attacks-trigger-raw-debate-on-immigration-in-germany-a-1071175.html
29 http://www.bbc.com/news/world-europe-35261988

domestic headlines for two weeks and was intensively reported elsewhere. The case impacted German policy and caused diplomatic tensions between Germany and Russia. Russian Foreign Minister Sergey Lavrov made two public concerns about the inability of the German police and legal system to take such cases seriously because of political correctness. The German authorities publicly accused Russia of interference in sovereign affairs, deliberate disinformation, and political propaganda.

As a result of different Russian activities, the new German White Book for security has identified Russia as one of the country's main challenges. According to its authors, the Russian leadership is not only questioning the post-Cold War security order in Europe, but it is also using "hybrid instruments for a targeted blurring of boundaries between war and peace" and "digital communication to influence public opinion" in Germany.[30]

Russia's threat perception and strategy

It is important to read, listen, and understand what the Russians are saying about the West. Russian strategists, intellectual elites, as well as the general public, are deeply convinced that the West is in a permanent struggle to keep Russia down.[31] The West (first and foremost the U.S. and the U.K.) is dedicated to dismantling Russian sphere of influence, certainly in Europe, the Baltics, the Balkans, the Middle East, Caucasus, and Central Asia. Russian strategists and intellectual elites consistently claim that the West invented a new type of indirect warfare and used it extensively after WWII. The central element is so-called information-psychological attacks on the masses.[32] The warfare that the West waged has reaped strategic successes for the past several decades, and the very collapse of the USSR - the biggest geopolitical disaster

30 www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

31 While original Russian sources are preferable PANARIN, I. N. 2008. *Informatsionnaia voina za budushchee Rossii | Информационная война за будущее России,* Moskva, Goriachaia liniia--Telekom., see a current review at: GILES, K., COLLEGE, N. D. & RESEARCH, D. 2016. *Handbook of Russian information warfare,* Rome, Italy, NATO Defence College Research Division.

32 THOMAS, T. 2014. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 27**,** 101-130.

of the century[33] - must only be the result of Western information warfare and other non-military efforts.[34] Overthrowing regimes in the USSR, its allies, and elsewhere, is possible through the use of Color Revolutions: seemingly spontaneous internal protests demanding regime change in targeted states. The argument is that Color Revolutions are not spontaneous uprising of masses against their leaders and institutions. Color Revolutions are the primary instrument of indirect warfare that the West wages. Like Western marketing, or public relations campaigns since the early days of capitalism, Color Revolutions are planned, designed and manufactured well in advance of their deployment. They begin as information campaigns, employing ideological, psychological, and information techniques to instigate antagonism in normal citizens.[35] This is the core driver of American "free Internet" ideology which contradicts territorial sovereignty – the foundation of the world order and international law. The American-pushed rise of online social media provides a unique tool to collect intelligence, as well as target and influence the minds of many unaware future protestors. Facebook, Twitter, and YouTube were used as PSYOP tools to carry out pro-American influence operations all over the world, sometimes with overt U.S. State Department support to large-scale protests. Non-violent appearance, attractive symbols, mass non-cooperation social disobedience and defiance of legitimate sovereign authority, are all crucial in Color Revolutions. Only when destabilization reaches a critical mass, swift seemingly organic violence versus disoriented defense forces is used to overthrow the regime.

Moreover, this non-linear/new-generation/hybrid[36] Western

33 https://www.youtube.com/watch?v=nTvswwU5Eco

34 PANARIN, I. N. 2010. Pervaia mirovaia informatsionnaia voina : razval SSSR | Первая мировая информационная война : развал СССР.

35 Vast effort is devoted by Russian academics and popular writers to study what they perceive as instruments of Western power, including: neuro-linguistic programming; subliminal messaging; psychotronic weapons; climate weapons; and other esoteric ideas often bordering conspiracy theories.

36 The terminologies used vary. *gibridnaya voyna* differs from Western Hoffman's' Hybrid War as discussed in:

FRIDMAN, O. 2017. Hybrid Warfare or Gibridnaya Voyna? *The RUSI Journal,* 162**,** 42-49. Fridman attributes the fact that *gibridnaya voyna* has very little in common with the Western, very military-oriented understanding

warfare is evolving and constantly applied in geostrategically advantageous areas against regimes unfriendly to American global dominance. Examples include Latin America, the Middle East, Asia, and, again - Russia and the former Soviet Republics (FSU) in the 21st century.[37] The Ministry of Defense's 2014 Moscow

---

of hybrid warfare to an intentional inaccuracy Russians introduced for political reasons.

See also:

GILES, K. 2016a. The next phase of Russian information warfare. Riga: NATO Strategic Communications Centre of Excellence. THOMAS, T. 2014. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 27**,** 101-130, THORNTON, R. 2015. The Changing Nature of Modern Warfare. *The RUSI Journal,* 160**,** 40-48, CHARLES, K. B. 2016. Russias Indirect and Asymmetric Methods as a Response to the New Western Way of War. *Special Operations Journal,* 2**,** 1-11. SEELY, R. 2017. Defining Contemporary Russian Warfare. *The RUSI Journal,* 162**,** 50-59, CZUPERSKI, M., HERBST, J., HIGGINS, E., POLYAKOVA, A. & WILSON, D. 2015. Hiding in plain sight : Putin's war in Ukraine. Atlantic Council of the United, States. CHAMBERS, J. & MODERN WAR, I. 2016. An analysis of Russia's 'new generation warfare' and implications for the US Army.

37 Monographs and edited volumes written in Russian are published commercially in Russia on the topic, and are quite popular reading reflecting the importance of the issue to Russian thinkers. See for example:

http://www.ozon.ru/?context=search&text=%f6%e2%e5%f2%ed%fb%e5+%f0%e5%e2%ee%eb%fe%f6%e8%e8+&group=div_book

http://www.ozon.ru/?context=search&text=%c3%e8%e1%f0%e8%e4%ed%e0%ff+%e2%ee%e9%ed%e0&group=div_book

http://www.ozon.ru/?context=search&text=%e8%ed%f4%ee%f0%ec%e0%f6%e8%ee%ed%ed%e0%ff+%e2%ee%e9%ed%e0&group=div_book

Academic sources are also popular (55 articles with Color Revolution in keywords published in Russian scientific journals since 2008 https://elibrary.ru/keyword_items.asp?keywordid=2989333). See:

TSYGANKOV, P. A. & ЦЫГАНКОВ, П. А. (eds.) 2015. *Gibridnye voiny" v khaotiziruiushchemsia mire XXI veka | Гибридные войны" в хаотизирующемся мире XXI века,* Moskva Издательство Московского университета, Moskva : Izdatel?stvo Moskovskogo universiteta, 2015. МОКШАНОВ, М. 2015. Актуальные вопросы противостояния гибридным войнам в условиях современной действительности. Наука. Мысль: электронный периодический журнал. ХАТУНОВ, С. Ю. & ПАВЛОВСКИЙ, А. И. 2016. Сетевой принцип организации «гибридной войны». Вопросы безопасности**,** 80-88. DEMIDOV, A. V. & ДЕМИДОВ, А. В. 2015. Стратегия «управляемого хаоса», как одно из проявлений политики «гибридных войн» [Hybrid Wars and Colour Revolutions: The Strategy of "Controlled Chaos" as One of the Symptoms of the Policy of

Conference on International Security identified Arab Spring as a wave of Color Revolutions.

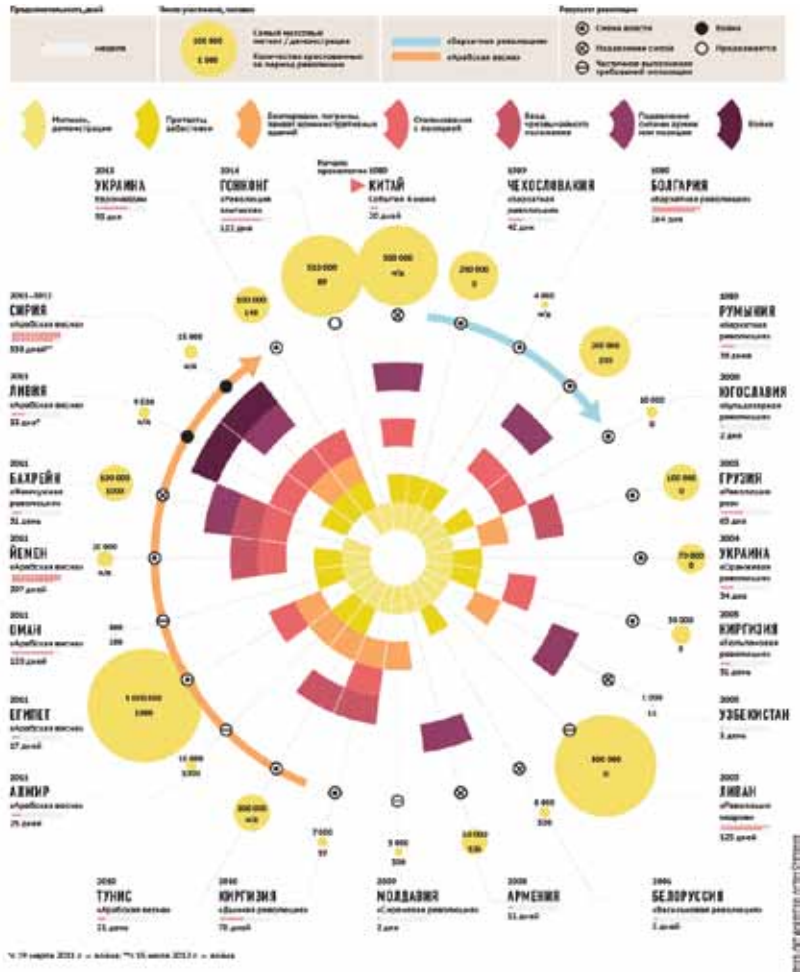

Figure 6: 24 Colour Revolutions since 1989. [38]

"Hybrid War"]. Геополитический журнал | Geopolitical Journal, 9, 16-20. БАРТОШ, А. А. & А., В. А. 2016. Применение гибридных методов в современных конфликтах | The Use of Hybrid Techniques in Modern Conflicts. Проблемы национальной стратегии, 39, 158-170.

38 http://oppps.ru/kak-delayut-cvetnye-revolyucii.html

If Color Revolutions fail, the West escalates the conflict to a "civil war", which sometimes requires Western "peacekeeping" force to intervene for "state-building," with the U.S. increasingly concealing its role by adopting the "leading from behind" strategy Obama used in Libya. According to the Russians, Western *gibridnaya voyna* erodes the socio-cultural cohesion of the adversary's population, ultimately leading to the replacement of an unfriendly regime by a Color Revolution, with minimum (if any) military intervention.[39] It incubates the US from the political and military risks associated with direct intervention, especially versus Russian nuclear deterrent.

As the then-president Dmitri Medvedev officially stated on the 22nd of February, 2011: *They [the West] prepared the same [Arab Spring] scenario for us before, and they will most certainly try it*.[40] Putin himself publicly accused then Secretary of State, Hillary Clinton, of running a massive long influence operation, first subverting Russian population and then fueling, and even sending "a signal" to the protesters that started in late 2011 in more than 70 cities across Russia.

Following the publication of the so-called Gerasimov doctrine,[41] the official Russian military doctrine, approved in December 2014, lists the key characteristics of modern conflicts: the use of information, political, and economic measures; the "protest potential" of the local population; and the use of special forces. All cause confusion and paralyze adversary's decision-making. Military force has a much smaller role than traditionally thought. Those strategy and techniques were used very successfully by Russia in Crimea,[42] less successfully in eastern Ukraine, and more forcefully in Syria.[43]

39 Fridman, O. (2017). "Hybrid Warfare or Gibridnaya Voyna?" The RUSI Journal 162(1): 42-49.

40 www.kremlin.ru/events/president/news/10408

41 CHARLES, K. B. 2016. Russias Indirect and Asymmetric Methods as a Response to the New Western Way of War. Special Operations Journal, 2, 1-11.

42 JAITNER, M. & MATTSSON, P. A. Russian Information Warfare of 2014. CyCon: International Conference on Cyber Conflict: Architectures in Cyberspace, 2015 Tallinn. 39-52. GEERS, K. (ed.) 2015. Cyber war in perspective : Russian aggression against Ukraine: Nato Cooperative Cyber Defence Centre of Excellence.

43 Israeli defense establishment started to pay attention to Russian doctrine only after acquiring intelligence from Syria on Russian actions.

Did Hostile Cybered Influence Operations yield influence?
Many Western popular and specialist discussions of Russian cybered influence operations give an impression that Russia is a determined, well-resourced and experienced adversary running the perfect campaign. The pertinent question remains: what will this campaign achieve?

MEASURES OF EFFECTIVENESS HAVE NOT BEEN PERFORMED
Having surveyed the Western discussion of the Russian cybered influence threat, the lack of scientifically valid measurement of effectiveness is striking. Most stakeholders assume effects, but none measure the supposed effects and validate the findings. To remind the reader: to measure effect, we need to reliably measure two different classes of phenomena: first the change in attitude, and then the change in actions.

- What are the initial attitudes targeted by the influence operation?
- Did the specific message/campaign reach the desired recipients in a timely manner?
- How many of the desired recipients engaged with the message?
- What part of the attention of the recipients did the message "win" versus competing or other messages out there and "noise"?
- Have the attitudes changed in the desired direction?
- Can attitude change be polled?
- Can attitude change be directly observed?
- Can attitude change be quantified?

All of the above are much easier to accomplish with the help of tools available to make sense of information people create and consume on online Social Media Platforms and Web browsing. Therefore, measuring attitudes seems to be simpler than measuring actions. What Measures of the Effectiveness (MoE) should be employed to assess the effect of these hostile Influence Operations? In business advertisement campaigns these are sales over time, but casual mechanisms are rarely demonstrated. In electoral campaigns these are the ballots, again casual mechanisms are rarely demonstrated. Other MoEs are collected through surveys, focus groups, online questionnaires,

opinion mining software tools and even consumer neuroscience, using Functional Magnetic Resonance Imaging (fMRI) and Event Related Potentials (ERP). These MoEs are directly applicable in the context of hostile Influence Operations, for measuring exposure to message. Legitimate domestic consumer and political marketing has consistently demonstrated the limited validity of these measures. Still, well-researched publications advocate to apply business marketing and advertising techniques to conflict areas as a useful framework for improving US military efforts to shape attitudes and behaviors of local populations. In particular, attention should be paid to "branding, customer satisfaction and segmentation of audiences."[44] The best dedicated political polling methods also failed by a very large margin to predict results in Israel's general elections, the UK Brexit vote, Italy's Renzi referendum, USA 2016 presidential election, and more. The logical conclusion is that if we were to apply domestic consumer and political marketing tools to the subject, we cannot expect reliable results.

The problem calls for a customized solution: issue-specific MoEs. Indeed even the American RAND corporation identified the absence of robust and empirical MOEs for military influence and PsyOps.[45] But developing valid and reliable MoEs on the basis of the existing tools for hostile influence operations conducted in civilian context is much more difficult. Maybe it is the reason for why the debates in Europe and the U.S. that I analyzed were devoid of fact-based measurements of effectiveness.

Moreover, the mix between attitudes and action seems to prevail in these debates. Let us assume for the sake of the argument that hostile cybered Influence Operations overcame the difficulties and indeed trigger the change in attitudes across the target audiences. Does that mean than perceptions will translate into political behavior? Can we assume that stronger anti-migrant opinion will directly cause violence against migrants and their supporters? Can we assume that isolationist anti-NATO and anti-

44 HELMUS, T. C., PAUL, C. & GLENN, R. W. 2007. Enlisting Madison Avenue: The marketing approach to earning popular support in theaters of operation, Rand Corporation. http://www.rand.org/pubs/monographs/MG607.html

45 U.S. Military Information Operations in Afghanistan Effectiveness of Psychological Operations 2001-2010. RAND 2012 http://www.rand.org/pubs/monographs/MG1060.html

EU sentiment will shift the electoral preferences of the public? The science of influence cautions against such an intellectual link. Nevertheless, numerous policy initiatives aired in conferences and media suggest that political and defense leaders assume that attitudes directly become behavior, in complete contradiction to scientific findings.

Conclusion

Western defense concerns regarding the cybered influence threat scenarios have both a theoretical foundation and empirical evidence. The stakes are high: defenders do not have the luxury to allow action for the sake of measurement. By the time actions are rolling – be it a rise of forces parties that oppose tolerance, EU, NATO and erode liberal values, or be it massive social unrest, protest, and erratic violence – it might be too late.

However, no data exists to assess the extent of impact and understand the mechanisms of cybered influence. The disturbing finding of my research is that no reliable measurement of the hostile Influence Operations via Social Media has been made public – nor has it probably ever been performed. My research findings cannot support the notion that defense authorities in European countries are utilizing the full extent of the possibilities available to assess the impact of Russian influence operations on target audience attitudes – let alone behavior. The belief that the cybered Influence Operations affect political behavior appears broad, but the means to measure this influence have remained largely ephemeral.

Cybered influence is a potent source and instrument of power	YES
Russia employs hostile cybered influence as a weapon, targeting democratic political processes in numerous Western societies	YES
Russia's cybered Influence Operations seriously threaten core Western interests	NO (we lack scientifically valid understanding of the effects)

The findings of my research reiterate what Rebecca MacKinnon writes:

we have a problem: we understand how power works in the physical world, but we do not yet have a clear understanding of how power works in the digital realm.[46]

My analysis of hostile cybered Influence Operations can be interpreted in several ways. Each one demands more research. The immediate call for action is for academic experts to work together with stakeholders that have access to the relevant data in order to systematically measure the impact of hostile cybered Influence Operations. Unless we jointly produce fact-based and scientifically valid understanding of the effects of hostile cybered Influence Operations, miscalculation and misaligned defense efforts, which may undermine the very liberties of our citizens, are the major risks for democracies as well as for NATO.

46 MACKINNON, R. 2013. Consent of the networked : the worldwide struggle for Internet freedom, New York, Basic Books.

References

2007. Field Manual FM 3–05.301 In: ARMY, D. O. T. (ed.) Psychological Operations Tactics, Techniques, and Procedures.

2014. Visual propaganda and extremism in the online environment, Carlisle, Pennsylvania, Stategic Studies Institute, United States Army War College Press.

CHAMBERS, J. & MODERN WAR, I. 2016. An analysis of Russia's 'new generation warfare' and implications for the US Army.

CHARLES, K. B. 2016. Russias Indirect and Asymmetric Methods as a Response to the New Western Way of War. Special Operations Journal, 2, 1-11.

CZUPERSKI, M., HERBST, J., HIGGINS, E., POLYAKOVA, A. & WILSON, D. 2015. Hiding in plain sight : Putin's war in Ukraine. Atlantic Council of the United, States.

DE MONTJOYE, Y.-A., RADAELLI, L., SINGH, V. K. & PENTLAND, A. S. 2015. Unique in the shopping mall: On the reidentifiability of credit card metadata. Science, 347, 536-539.

DEMIDOV, A. V. & ДЕМИДОВ, А. В. 2015. Стратегия «управляемого хаоса», как одно из проявлений политики «гибридных войн» [Hybrid Wars and Colour Revolutions: The Strategy of "Controlled Chaos" as One of the Symptoms of the Policy of "Hybrid War"]. Геополитический журнал | Geopolitical Journal, 9, 16-20.

EXCELLENCE, N. S. C. C. O., SVETOKA, S. & REYNOLDS, A. 2016. Social media as a tool of hybrid warfare.

FRIDMAN, O. 2017. Hybrid Warfare or Gibridnaya Voyna? The RUSI Journal, 162, 42-49.

GEERS, K. (ed.) 2015. Cyber war in perspective : Russian aggression against Ukraine: Nato Cooperative Cyber Defence Centre of Excellence.

GILES, K. 2016a. The next phase of Russian information warfare. Riga: NATO Strategic Communications Centre of Excellence.

GILES, K. 2016b. Russia's 'new' tools for confronting the west : continuity and innovation in Moscow's exercise of power. In: RUSSIA & EURASIA, P. (eds.). London: The Royal Institute of International Affairs Chatham House.

GILES, K., COLLEGE, N. D. & RESEARCH, D. 2016. Handbook of Russian information warfare, Rome, Italy, NATO Defence College Research Division.

GLADWELL, M. 2002. The tipping point : how little things can make a big difference, Boston, Back Bay Books.

HELMUS, T. C., PAUL, C. & GLENN, R. W. 2007. Enlisting Madison Avenue: The marketing approach to earning popular support in theaters of operation, Rand Corporation.

JAITNER, M. & MATTSSON, P. A. Russian Information Warfare of 2014. CyCon: International Conference on Cyber Conflict: Architectures in Cyberspace, 2015 Tallinn. 39-52.

KUEHL, D. T. 2009. Cyberspace and Cyberpower. In: KRAMER, F. D., STARR, S. H. & WENTZ, L. K. (eds.) Cyberpower and national security. National Defense University Press : Potomac Books.

KUHN, T. S. 1962. The structure of scientific revoutions, Chicago, The University of Chicago Press.

LAPIERE, R. T. 1934. Attitudes vs. Actions. Social Forces, 13, 230-237.
LUCAS, E. 2015. Cyberphobia: identity, trust, security and the Internet, Bloomsbury Publishing.
MACKINNON, R. 2013. Consent of the networked : the worldwide struggle for Internet freedom, New York, Basic Books.
MAYER, J., MUTCHLER, P. & MITCHELL, J. C. 2016. Evaluating the privacy properties of telephone metadata. Proceedings of the National Academy of Sciences, 113, 5536-5541.
MURRAY, W. & MANSOOR, P. R. 2012. Hybrid warfare: fighting complex opponents from the ancient world to the present, Cambridge University Press.
NYE, J. S. 1990. Soft power. Foreign policy, 153-171.
NYE, J. S. 2010. Cyber Power, Belfer Center for Science and International Affairs; Harvard Kennedy School.
PANARIN, I. N. 2008. Informatsionnaia voina za budushchee Rossii | Информационная война за будущее России, Moskva, Goriachaia liniia--Telekom.
PANARIN, I. N. 2010. Pervaia mirovaia informatsionnaia voina : razval SSSR | Первая мировая информационная война : развал СССР.
POPPER, K. R. 1965. The logic of scientific discovery, New York, Harper & Row.
POPPER, K. R. 1972. Objective knowledge : an evolutionary approach, Oxford, The Clarendon Press.
SEELY, R. 2017. Defining Contemporary Russian Warfare. The RUSI Journal, 162, 50-59.
THOMAS, T. 2014. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? The Journal of Slavic Military Studies, 27, 101-130.
THORNTON, R. 2015. The Changing Nature of Modern Warfare. The RUSI Journal, 160, 40-48.
TSYGANKOV, P. A. & ЦЫГАНКОВ, П. А. (eds.) 2015. Gibridnye voiny" v khaotiziruiushchemsia mire XXI veka | Гибридные войны" в хаотизирующемся мире XXI века, Moskva Издательство Московского университета, Moskva : Izdatel'stvo Moskovskogo universiteta, 2015.
WINEBURG, S., MCGREW, S., BREAKSTONE, J. & ORTEGA, T. 2016. Evaluating Information: The Cornerstone of Civic Online Reasoning. Stanford university.
БАРТОШ, А. А. & А., В. А. 2016. Применение гибридных методов в современных конфликтах | The Use of Hybrid Techniques in Modern Conflicts. Проблемы национальной стратегии, 39, 158-170.
МОКШАНОВ, М. 2015. Актуальные вопросы противостояния гибридным войнам в условиях современной действительности. Наука. Мысль: электронный периодический журнал.
ХАТУНОВ, С. Ю. & ПАВЛОВСКИЙ, А. И. 2016. Сетевой принцип организации «гибридной войны». Вопросы безопасности, 80-88.

Previous publications in this series:

1-2017 Samhandling for sikkerhet – En ny sikkerhetslov for en ny tid ***Kim Traavik***
3-2016 Erdoğan's Turkey: An Unpredictable Partner for a Desperate EU? ***Joakim Parslow***
2-2016 Ten Proposition about the US and the Middle East ***Steven Simon***
1-2016 The Migration Challenge from MENA: considering the EU`s struggles ***James H. Wyllie***
4-2015 A Timeline for the Conflict and War in Ukraine ***Geir Flikke and Tor Bukkevold***
3-2015 Opening speech at the 2015 Leangkollconference ***Erna Solberg***
Prospects for NATO–Russia relations ***Alexander Vershbow***
2-2015 Fremveksten av autonome droner ***Gjert Lage Dyndal***
1-2015 Crimea and the Russian-Ukrainian conflict ***Anton Alex Bebler***
3-2014 Baltikum, Russland og fremtiden ***Tor Husby***
2-2014 Russlands stormaktsstrategi og Vestens respons ***Janne Haaland Matlary***
1-2014 What now, little England? Prospects for the forthcoming Scotland and EU referendums. ***Øivind Bratberg***
4-2013 Konflikten i Syria ***Rolf Willy Hansen***
3-2013 Polen – et lyspunkt i Europa ***Jahn Otto Johansen***
2-2013 Hva skjer i Nord-Korea – Asiatisk stabilitet i fare? ***Sverre Lodgaard***
1-2013 Engaging with Islamists: A new agenda for the policy community ***Mona Kanwal Sheikh***
3-2012 US Shale Oil Revolution and the geopolitics of Oil ***Trygve Refvem***
2-2012 NATO's influence in the near abroad ***Oktay Bingöl***
1-2012 Ungarn – alene og miskjent ***Jahn Otto Johansen***
4-2011 Conflict or Coincidence of Interest of Main Oil and Gas Importing, Exporting and Transit Countries ***Liana Jervalidze***
3-2011 Breaking down the remaining walls ***Alister Miskimmon***
2-2011 Russia in NATO ***Charles A. Kupchan***
1-2011 Bringing War Home–The use of Provincial Reconstruction Teams by Norway and Denmark to construct strategic narratives for their domestic audiences ***Ida Dommersnes***
5-2010 Sjøforsvarets historie 1960-2010–En kortversjon ***Roald Gjelsten***
4-2010 The Tragedy of small power politics Asle Toje
3-2010 Integrasjon med grenser eller grenseløs integrasjon? ***Bjørn Innset***
2-2010 Reconciling the nuclear renaissance with disarmament Alex Bolfrass and ***Kelsey Hartigan***
1-2010 Approaching the comprehensive approach ***Dag Kristiansen***
3-2009 Turkish Neo-Ottomanism: A turn to the Middle East? ***Einar Wigen***
2-2009 20 år etter muren ***Jahn Otto Johansen***
1-2009 Between Reluctance and Necessiy: The Utility of Military force in Humanitarian and Development Operations ***Robert Egnell***
5-2008 Civil-military relations: No Room for Humanitarianism in comprehensive approaches ***Stephen Cornish and Marit Glad***
4-2008 Tsjekkoslovakia–40 år etter ***Jahn Otto Johansen***
3-2008 NATO–Moldova/Israel/Ukraine ***Dr. Gabanyi, Dr.Kogan, Dr. Begma & Igor Taburets***
2-2008 Hearts, minds and guns: the Role of the Armed Forces in the 26st Century ***UK Chief of Defence Staff, Air Chief Marshal Sir Jock Stirrup***
1-2008 Krav til fremtidens forsvar sett fra unge offiserers ståsted ***Tomas Bakke, Kadett Krigsskolen***
7-2007 Threats to Progress of Democracy and Long Term Stability in Georgia ***Liana Jervalidze***
6-2007 Militærmaktens særtrekk i moderne konflikter ***Div. forfattere***
5-2007 Norge i et Sikkerhetspolitisk Dilemma ***Asle Toje***
5-2007 EU-staters varierende bidragsvilje til militær intervensjon ***Rolf Magnus Holden***
4-2007 Defence as the Best Offence? Missile Defences and Nuclear Non-proliferation ***Lars Van Dassen and Morten Bremer Mærli***
3-2007 Putins Russland–Partner eller utfordrer? ***Jahn Otto Johansen***
2-2007 Energy and Identity–Readings of Shtokman and NEPG ***Jakub M. Godzimirski***
1-2007 NATO and the Dialouge of Civilisations ***Christopher Cooker***
1-2007 NATO planlegger å være relevant–også i fremtiden ***Ivar Engan***

6-2006 Ungarn 1956–Et 50-årsminne ***Jahn Otto Johansen***

5-2006 NATO foran toppmøtet i Riga ***Ambassadør Kai Eide***

4-2006 Russian energy policy and its challenge to western policy makers ***Keith Smith***

4-2006 Oil and gas in The High North–A percpective from Norway ***Ole Gunnar Austvik***

2-2006 EUs sikkerhetspolitiske rolle i internasjonal politikk ***Jan Erik Grindheim***

1-2006 Fra "Kursk" til "Priz": Ubåtredning som internasjonalt samarbeidsområde ***Kristian Åtland***

9-2005 Nordisk sikkerhet ***Tønne Huitfeldt***

8-2005 NATO going global or almost

The Current Revolution in the Nature of Conflict

The Fiftieth Anniversary of the Norwegian Atlantic Committee. ***Alv Jakob Fostervoll, Jamie Shea, Chris Donnelly***

7-2005 Galileo–et europeisk globalt navigasjonssystem ***Hans Morten Synstnes***

6-2005 Coming home to Europe? Central and Eastern Europe in EU and NATO

Eastern Europe's silent revolution ***Jahn Otto Johansen og Nils Morten Udgaard***

5-2005 Det tyske eksperiment ***Jahn Otto Johansen***

4-2005 The naval Dilemma of the early 26st Century ***Hans Olav Stensli***

3-2005 What are the strategic challenges faced by Norway in the years to come?

In the new types of conflict we face, how to define and defend humanitarian space?

The Norwegian Atlantic Committee's 40th annual Leangkollen Conferance. the Nobel Institute. ***Jørgen Kosmo and Jonas Gahr Støre***

2-2005 The New Geopolitics of the North? ***Jakub M. Godzimirski***

1-2005 "Global Partnership", russiske ubåter og brukt kjernebrensel – internasjonal koordinering av oppgaver og bidrag ***Christina Chuen og Ole Reistad***

6-2004 Oljens geopolitikk og krigene ved Persiagulfen ***Ole Gunnar Austvik***

5-2004 Coping with Vulnerabilities and the Modern society ***Jan Hovden***

4-2004 Forsvarsperspektiver i nord ***Jørgen Berggrav***

3-2004 NATO og de transatlantiske motsetninger

-Kortsiktige og langsiktige perspektiver ***Jahn Otto Johansen***

2-2004 The Role of a Humanitarian Organization in an International Security Operation -

a Basis for Cooperation or a Basis for Separation? ***Jonas Gahr Støre***

1-2004 If Effective Transatlantic Security Cooperation is the Question, Is NATO the Answer? ***Stanley R. Sloan***

6-2003 Frankrike og Irak-krigen: Bare i prinsippenes navn? ***Frank Orban***

5-2003 Norwegian Priorities for the Extended G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction ***Asle Toje and Morten Bremer Mærli, NUPI***

4-2003 Saddam's Power Base ***Major John Andreas Olsen***

3-2003 Terroristbekjempelse og folkeretten ***Terje Lund***

2-2003 Men and Machines in Modern Warfare ***General Charles A. Horner (ret.)***

1-2003 The Real Weapon of Mass Destruction: Nuclear, biological and chemical warfare in the era of terrorism and "rogue" states ***Morten Bremer Mærli***

www.dnak.org

B ØKONOMI ÉCONOMIQUE

NORGE P. P. posten

DEN NORSKE ATLANTERHAVSKOMITE
THE NORWEGIAN ATLANTIC COMITTEE

Fridtjof Nansens plass 8
N-0160 Oslo
Tel: +47 22 40 36 00
Fax: +47 22 40 36 10
post@dnak.org
www.dnak.org